Dr. Courtney N. Phillips, Executive Commissioner

Statement of Work ("SOW")

TIERS Cloud Assessment and Migration Planning Services
SOW No. HHS0006347

DIR DBITS Category: Technology Migration/Upgrade

Date of Release: 11/22/2019
Responses Due: 12/21/2019

NIGP CODE: 920-05

Table of Contents

ARTICLE I. EXECUTIVE SUMMARY, DEFINITIONS, AND AUTHORITY 4

1.1. EXECUTIVE SUMMARY 4
1.2. DEFINITIONS 4
1.3. AUTHORITY 5
1.4. BACKGROUND 5

ARTICLE II. SCOPE OF WORK 6

2.1. DESCRIPTION OF SERVICES/STATEMENT OF WORK/SPECIFICATIONS 6
2.1.1. Summary of Services 6
2.1.2. Cloud Migration Constraints 7
2.1.3. Project Phases 8
2.1.4. Deliverables 15
2.1.5. Progress Reporting 18
2.1.6. Vendor Responsibilities 18
2.1.7. HHSC Responsibilities 19
2.1.8. Work Products 19
2.1.9. Invoicing 20
2.1.10. Service Level Agreements (SLAs) 21
2.2. CONTRACT AWARD AND TERM 21
2.2.1. Contract Award and Execution 21
2.2.2. Contract Term 21
2.3. DATA USE AGREEMENT AND SECURITY AND PRIVACY INITIAL INQUIRY 22

ARTICLE III. ADMINISTRATIVE INFORMATION 22

3.1. SCHEDULE OF EVENTS 22
3.2. CHANGES, AMENDMENT OR MODIFICATION TO SOLICITATION 22
3.3. IRREGULARITIES 23
3.4. INFORMALITIES 23
3.5. INQUIRIES 23
3.5.1. Point of Contact 23
3.5.2. Questions 23
3.5.3. Prohibited Communication 24
3.5.4. Clarification 24
3.5.5. Responses 24
3.6. PROPOSAL COMPOSITION 24
3.6.1. General 24
3.6.2. Submission in Separate Parts 25
3.6.3. Page Limit and Supporting Documentation 25
3.6.4. Discrepancies 25
3.6.5. Exceptions 25
3.6.6. Assumptions 26
3.7. PROPOSAL SUBMISSION AND DELIVERY 26
3.7.1. Deadline 26
3.7.2. Labeling 26
3.7.3. Delivery 26
3.7.4. Alterations, Modifications, and Withdrawals 27

ARTICLE IV. PROPOSAL EVALUATION AND AWARD PROCESS 28

4.1. EVALUATION CRITERIA 28
4.1.1. Vendor Qualifications 28
4.1.2 Minimum Qualifications 28
4.1.3 Specific Criteria 28
4.1.4 Other Information 29
4.2. INITIAL COMPLIANCE SCREENING 29
4.3. COMPETITIVE RANGE AND BEST AND FINAL OFFER 29
4.4. ORAL PRESENTATIONS AND SITE VISITS 29
4.5. QUESTIONS OR REQUESTS FOR CLARIFICATION BY THE HHSC 29

ARTICLE V. NARRATIVE PROPOSAL 30

5.1. EXECUTIVE SUMMARY 30
5.2. PROJECT APPROACH 30
5.3. STAFFING PLAN 31
5.4. PROJECT WORK PLAN 31
5.5. EXAMPLE WORK PRODUCTS 31

ARTICLE VI. REQUIRED RESPONDENT INFORMATION 33

6.1. COMPANY INFORMATION 33
6.1.1. Company Narrative 33
6.1.2. Company Profile 33
6.2. PAST PERFORMANCE 33
6.3. MAJOR SUBCONTRACTOR INFORMATION 33
6.4. LITIGATION AND CONTRACT HISTORY 33
6.5. CONFLICTS OF INTEREST 34
6.6. AFFIRMATIONS AND CERTIFICATIONS 34
6.7. FINANCIAL SECURITY 34
6.8. HUB SUBCONTRACTING PLAN 35

ARTICLE VII. COST PROPOSAL 35

7.1. COST PROPOSAL 35

ARTICLE VIII. GENERAL INFORMATION 36

8.1. GENERAL INFORMATION 36
8.1.1. Amendment 36
8.1.2. Offer Period 36
8.1.3. Costs Incurred 36
8.1.4. Contract Responsibility 36
8.1.5. Public Information Act 36
8.2. PROTEST 37

ARTICLE IX. SUBMISSION CHECKLIST 38

ARTICLE X: EXHIBITS AND ATTACHMENTS 40

ARTICLE I. EXECUTIVE SUMMARY, DEFINITIONS, AND AUTHORITY

1.1. EXECUTIVE SUMMARY

The Texas Health and Human Services Commission ("HHSC"), seeks a qualified Vendor to provide Cloud Assessment and Migration Planning Services for the HHSC Texas Integrated Eligibility Redesign System ("TIERS"). The purpose of these Services is to assist HHSC in planning the migration of the TIERS and Eligibility Supporting Technologies ("EST") applications to the cloud. This includes developing a recommended framework that takes full advantage of cloud best practices and enabling the transformation of TIERS from a monolithic architecture to a services/micro-services architecture. The primary goal of this project is to prepare HHSC to move the TIERS and EST applications to the cloud which will result in improvements in efficiency, agility, and innovation.

The HHSC Information Technology Social Services Applications ("IT-SSA") organization will provide oversight of the awarded Contract and the services provided in accordance with the SOW. The terms and conditions of this SOW may not, and shall not be construed to, weaken any terms and conditions in Vendor's DIR Contract. To the extent that any terms and conditions of this SOW are less rigorous than or otherwise diminish Vendor's obligations under the DIR Contract, the terms and conditions of the DIR Contract supersede and control over this SOW. The terms and conditions of this SOW may, however, add to or strengthen the terms and condition under Vendor's DIR Contract. To the extent that any HHSC terms and conditions add to or strengthen Vendor's obligations, the HHSC terms and conditions control.

For award consideration, Respondents must execute **Exhibit B - HHSC Affirmations and Solicitation Acceptance, Exhibit E1 - Federal Assurances – Non Construction** and provide all other required information and documentation as set forth in this SOW.

1.2. DEFINITIONS

Refer to **Exhibit C1 - HHSC Uniform Terms and Conditions**, and **Exhibit C2 - HHSC Special Conditions**, for additional definitions.

Additionally, as used in this Solicitation, unless the context clearly indicates otherwise, the following terms and conditions have the meanings assigned below:

Health and Human Services Commission or HHSC - means the administrative agency established under Chapter 531, Texas Government Code or its designee.

HUB - means Historically Underutilized Business, as defined by Chapter 2161 of the Texas Government Code.

HUB Subcontracting Plan or HSP means written documentation regarding the use of subcontractors, which is required to be submitted with all responses to state agency Contracts with an expected value of $100,000 or more where subcontracting opportunities have been determined by the state agency to be probable. The HUB subcontracting plan subsequently becomes a provision of the awarded Contract and is monitored for compliance by the state agency during the term of the Contract.

Respondent - means the Vendor entity responding to this Solicitation.

SOW - means this Statement of Work including any Exhibits and Addenda, if any.

State - means the State of Texas and its instrumentalities, including HHSC, and any other state agency, its officers, employees, or authorized agents.

1.3. AUTHORITY

HHSC is soliciting the services listed herein under Title 10, Subtitle D of the Texas Government Code, in particular Texas Government Code, §2155.144 and §2157.068.

1.4. BACKGROUND

The mission of HHSC is to administer all Health and Human Services programs in Texas using the highest standards of service, transparency, and accountability for the effective use of funds. **Attachment A – HHSC and TIERS Background Information** provides an overview of HHSC and the HHSC Information Technology organizations.

TIERS is the integrated eligibility system managing delivery of one hundred sixty-four (164) types of assistance including food, cash, medical, and community care services to Texans in need. Over 10,000 unique users rely on TIERS every day. TIERS automates complex rule-based processing ensuring consistency in eligibility determination, serving around five and half million (5,500,000) recipients annually. TIERS is a mission critical system for HHSC and for the State of Texas.

The TIERS Ecosystem consists of numerous integrated interrelated applications and business functions. The technical aspect of the TIERS system consists of a collection of information systems spanning multiple platforms. These systems include the TIERS and EST applications. **Attachment B – TIERS and EST Application Overview** provides a description of the TIERS Ecosystem, the TIERS & EST applications, and the technical tools employed to support TIERS. **Attachment C – TIERS Functional and Architecture Overview** provides a summary of the TIERS business processes, the TIERS hosting environment, and the TIERS architecture. HHSC is in the initial phase of readying TIERS applications, data, and work processes for migration to the cloud.

The purpose of this SOW is to assist HHSC in planning the migration of the TIERS and EST applications to the cloud. This includes developing a recommended framework that takes full advantage of cloud best practices and enabling the transformation of TIERS from a monolithic architecture to a services/micro-services architecture. The primary goal of this project is to prepare HHSC to move the TIERS and EST applications to the cloud which will result in improvements in efficiency, agility, and innovation.

ARTICLE II. SCOPE OF WORK

2.1. DESCRIPTION OF SERVICES/STATEMENT OF WORK/SPECIFICATIONS

2.1.1. SUMMARY OF SERVICES

The Vendor shall provide services to support HHSC desired assessment, including:

1. Comprehensive analysis and understanding of the current environment, and analysis of which on-premises technical resources are best suited for the cloud.
2. Comprehensive planning for migration to the cloud that supports cost-effective, secure, resilient, and agile IT management.
3. Successful and complete transition of specified applications, solutions, and services to the cloud, in compliance with HHS IT Policy.
4. Consolidated and simplified application, service management, data management, Development Security Operations ("DevSecOps") and monitoring in the cloud to support cost-effective, secure, and agile IT management.
5. Successful decommissioning of specified applications, solutions, and services within 18 months of the solution go-live.
6. Efficient and policy compliant disposition of unneeded data center assets.

The Vendor's services will consist of one or more of the following:

1. Determining the current TIERS inventory of items that may be impacted by the cloud migration.
2. Assessing the current environment to determine which application and processing workloads are suitable for migration.
3. Determining the service and deployment models including a streamlined application development strategy (e.g. Continuous Integration/ Continuous Delivery (CI/CD) pipeline).
4. Developing the business case.
5. Assessing security risks and impacts of the migration.
6. Developing the Cloud Migration Strategy and Plan.
7. Developing the Data Center Decommissioning Plan.

These services will list all capabilities necessary to effectively support:

1. Cloud migration;
2. Validation of readiness, solutions, and applications;
3. Analysis of current service contracts, maintenance contracts, data circuit agreements, and asset tracking elements to identify gaps and provide associated

recommendations to support cost-effective, secure, resilient, and agile IT management for cloud migration.

2.1.2. CLOUD MIGRATION CONSTRAINTS

The TIERS applications are considered business critical because they are essential in providing public assistance benefits every day to Texas residents in need. Towards this end, during the migration of the application and services, the expectation is that all business functions will be available with minimal downtime. The Respondent shall provide an assessment to support desired outcomes within the following operational constraints, including but not limited to:

2.1.2.1. MINIMAL DISRUPTION

1. Portability/Interoperability: Portability and interoperability alternatives across supporting services like identity and access management, vendor/third party connectivity, on-premises systems, hybrid/ multi cloud connectivity, etc. to allow for ease of transition to the desired HHSC/TIERS cloud migration end state should be maintained.

2. Legacy system and data center decommissioning time line: Legacy systems should be maintained and operational during transition along with cloud migration solutions to support ongoing development of business requirements as per business roadmaps in legacy systems and support for transition to cloud-based solutions.

2.1.2.2. COST IMPACTS

1. Vendor service agreements: Service Level Agreements ("SLAs") on legacy systems' maintenance, monitoring and operational efficacy should be maintained and considered during the transition phase.

2. Licensing requirements: Software, tools and COTS licensing contracts and requirements on legacy systems should be factored into the transition.

2.1.2.3. DATA SENSITIVITY

1. Application or service data sensitivity details such as Protected Health Information ("PHI") or Personally Identifiable Information ("PII") should be considered during transition and after, to allow HHSC to meet state and federal mandates in data privacy laws. HHSC's security standards for confidential information should be maintained during transition including federal standards like Federal Information Processing Standards ("FIPS") and National Institute of Standards and Technology ("NIST") Special Publications regulations.

2. Data exchange with dependent applications should continue in a secure manner during and after migration.

2.1.2.4. OPERATIONAL PROCESSES

1. Monitoring: Monitoring processes of legacy and (multi) cloud transitioned applications and services should be updated to assist with the transition. These processes should help maintain currents SLAs. HHSC must have access to data

required to maintain SLAs defined by TIERS Applications and Data Center Services.

2. Mean Time to Resolution: Help Desk, outage review, and analysis processes should provide support for legacy and transitioned services to maintain current mean time to resolution.

3. Disaster Recovery: Disaster recovery risks should be minimized with updated processes for migrated systems/services and integration with legacy systems and services.

2.1.2.5. PERFORMANCE

1. Geographically distributed offices should continue to have the same level or better performance during the cloud strategy implementation.

2. Network, storage and other infrastructure components should continue to perform as per defined SLAs.

2.1.3. PROJECT PHASES

The selected Vendor will conduct the project based on the following phases and requirements.

2.1.3.1. PHASE 1 – TIERS INVENTORY

1. Prepare a TIERS inventory that includes: Users (see Attachment A), Applications, Infrastructure, Technology Resources, Security Requirements, Processes, and Service Management.

2. Utilize industry best practices to conduct an inventory of IT assets to provide a comprehensive view of HHSC's applications, infrastructure and security.

3. Produce thorough analysis resulting in a comprehensive report on HHSC's IT Users and End User stakeholders that would be impacted by cloud migration. For example, stakeholder groups could include Executive Sponsor, Legal & Contracts Management, Business Units, Applications, Infrastructure, Security, Help Desk and End User stakeholders.

4. Identify the business processes and governance processes that are associated with current inventory (both applications and infrastructure).

5. Produce a baseline of HHSC's technical environment including inventory of both infrastructure and applications, to include development/testing environments.

6. Prepare an inventory of the current infrastructure such as hardware, application, middleware & databases, networks, as well as any other relevant factors or components of the infrastructure.

2.1.3.2. PHASE 2 – TIERS CLOUD ASSESSMENT

1. Map applications including dependencies and data flows.

2. Conduct a suitability analysis, identifying appropriate service models (e.g. Infrastructure as a Service ("IaaS") and deployment models (e.g. public or hybrid cloud)).
3. Provide recommendations for a specific cloud service model (e.g. containerization using orchestration technology, disparate VM without containers, server-less, etc.,).
4. Developing the business case to quantify cost and benefits. (e.g. workload shift to cloud vendor, reducing procurement time and reducing cost.)
5. Provide recommendations on application architecture which is best suited for the recommended cloud service model (e.g. event-driven micro-services, service-oriented architecture) or whether an application's architecture should remain the same.
6. Provide summaries of key results, analysis, and recommendations to improve HHSC leadership, customer, and legislator's understanding of the benefits and implications of moving individual TIERS applications or groups of TIERS applications to the cloud.
7. Produce "quick win" analysis of applications that are well-suited for accelerated deployment to the cloud and provide recommendations for executing this migration.
8. Provide technical services for application mapping including illuminating interdependencies such as application dependencies and affinities to servers, server configuration etc.
9. Identify how any changes to the applications or their deployment will affect interfaces with enterprise services (e.g. authentication and authorization).
10. Identify and document critical dependencies between applications and data.
11. Develop application evaluation criteria, application profiling, and application dependency mapping, including criteria for mapping multi-purpose applications.
12. Identify and describe the methodology for analyzing applications/infrastructure across a range of lifecycle stages (e.g. development, testing, and production).
13. Identify the approach for decomposition of applications and identification of common functions and services that can potentially be migrated to the cloud, and identification of potential shared services.

2.1.3.3. PHASE 3 – APPLICATION TRANSFORMATION PLANNING

1. Identify application changes (e.g. refactoring, rewriting, shared services, etc.) to enable HHSC to maximize cloud benefits (e.g. horizontal scaling, server-less computing, etc.).
2. Identify technologies to improve time to delivery (e.g. fully automated DevSecOps pipeline to support CI/CD and software defined data center).

3. Identify technologies that prevent migrating to the cloud and recommend appropriate cloud services/open source replacements.
4. Identify technologies that significantly reduce the benefits of moving to the cloud and recommend appropriate cloud services/open source replacements.
5. Recommend strategies that maximize cloud benefits and prevent/minimize cloud vendor lock-in.
6. Assess DevSecOps maturity and recommend improvements.
7. Assess current state architecture standards and provide recommendations.
8. Identify and assess application transformation requirements that identify TIERS applications that need refactor or rewrite to achieve maximum efficiency and benefits of the cloud.
9. Identify and assess environment and infrastructure changes necessary to support application transformation (i.e. container adoption, shared services, or micro-services, etc.).
10. Identify and assess a strategy for transforming the TIERS database environment to cloud-ready/cloud-native database(s).
11. Identify and assess licensing concerns and provide recommendations for transitioning/reducing current licenses to support the cloud.
12. Identify and assess current TIERS data management strategy and provide recommendations for automation, analytics, data retention, reporting, standardization and categorization to support the cloud.

2.1.3.4. PHASE 4 – CLOUD SECURITY PLANNING

1. Provide a comprehensive analysis of current applications and infrastructure for security and privacy requirements such as data sensitivity, legal or other regulatory issues, disaster recovery, multi-factor authentication, currently deployed remote access or internal security considerations, etc. that potentially impact the migration.
2. Identify how applicable security and privacy provisions of the Federal Risk and Authorization Management Program ("FedRAMP") standardized security assessment, authorization, and continuous monitoring policies impact the migration and provide recommendations.
3. Identify how applicable security provisions of the CMS Minimum Acceptable Risk Standards for Exchanges ("MARS-E"), the Texas HHS Information Security Controls and any other state regulations impact the migration and provide recommendations, especially with respect to the on-going reassessment of TIERS security compliance with the provisions. Refer to the following attachments for additional information:
    a. Attachment E – Texas HHS Information Security and Privacy Requirements for TIERS Data Center Services

i. Note: Attachment E contains the security and privacy requirements for TIERS Data Center Services *only*. Establishing security and privacy requirements relative to the complete TIERS ecosystem is part of the on-going reassessment of TIERS.

b. Attachment F – HHS Information Security (IS Controls) v1.0

c. Attachment G - Information Security Assessment Supplemental Guidance for External Entities

4. Identify how applicable Administrative, Operational, and Security provisions and guidelines outlined in the FIPS and NIST Special Publications regulations impact the migration, and provide recommendations.

5. Identify how applicable provisions within the NIST Special Publication 800-144 – "Guidelines on Security and Privacy in Public Cloud Computing" or other applicable standards and guidelines impact the migration and provide recommendations.

6. Recommend an active and ongoing compliance program that provides evidence of compliance with applicable security controls and Privacy and Risk Impact Assessments.

7. Develop and describe the framework and approach to incorporating both federal and agency security requirements into migration planning recommendations.

8. Identify security and privacy standards to which the migration plan should conform, including:

   - HHS Information Security Controls
   - Properly securing the connections between formerly co-located systems, including systems not migrated for business or other reasons.
   - Implementation of trusted internet connections and similar mandates.
   - Implementation of HHSC's intellectual property rights as referenced in **Exhibit C1 - HHSC Uniform Terms and Conditions**.

9. Provide recommendations for a security plan focused on the integration points of end-user authentication (e.g. Active Directory, LDAP), cloud environment management authentication, physical and logical segmentation based on requirement per data type and certification (e.g. FedRAMP) delivering a single comprehensive solution that can be leveraged across the organization reducing end user confusion and security management complexity.

10. Provide requirements for security for non-standard data transfers both in transit and at rest resulting from the migration of the applications or services to the cloud in compliance with FIPS 140-2 requirements.

11. Provide recommendations for demonstrating cloud migration compliance with the most current version of the State's security policies and standards.

12. Develop plans and solutions that utilize State designated time servers using Network Time Protocol ("NTP") where time server references are required in the cloud service provider's physical and virtual infrastructure.

13. Provide processes that ensure no administrative or other credentials are shared and that access to root, administrative or super user privileges are not achieved via shared credentials during the migration.

14. Provide recommendations for adjusting the current TIERS continuous monitoring program and dashboards to maintain compliance with NIST SP 800-137, Information Security Continuous Monitoring, detailed contractually, and address at a minimum required updates to the authorization based on any significant changes to the Cloud Service Provider ("CSP") environment, address new state and Federal requirements, and provide updates to control implementations on a basis frequent enough to make on-going risk-based decisions.

15. Provide recommendations for IPv6 in support of the Civilian Agency Acquisition and Defense Acquisition Regulations Council.

16. Collaborate with HHSC IT Apps and CISO organizations to support and advise regarding clear security authorization requirements by analyzing and classifying the data to be placed in the cloud and categorizing the system data according to HHS Information Security Controls requirements. Provide recommendations on the security impact level a CSP environment must meet based on the data characterizations, and what specific security controls must be implemented to ensure a CSP environment meets the security needs of the agency.

17. Identify how applicable provisions within CMS and HHS Agency's Computer Security Incident Handling Guides, including accountability for incident response responsiveness, providing specific time frame for restoration and secure services in the event of an incident impact the migration and provide recommendations.

18. Provide recommendations for key escrow, if required.

19. Identify how applicable provisions within CMS and HHS data retention and audit requirements impact the migration and provide recommendations.

20. Identify and provide recommendations regarding potential impacts to the TIERS System Security Plan ("SSP") complete with defined authorization boundaries resulting from the cloud migration.

2.1.3.5. PHASE 5 – CLOUD MIGRATION PLANNING

1. Provide migration planning, including developing a multi-step migration roadmap.

2. Recommend/design the environment for testing cloud applications or services.

3. Produce a roadmap for HHSC to effectively plan for cloud migration that maximizes cost reduction and identifies constraints and inhibitors to cloud migration.

4. Provide maximum alignment to State of Texas and HHSC cloud objectives (e.g., State Strategic Plan for Information Resource Management), mandates, and requirements to amplify HHSC's ability to achieve legislative and strategic objectives.
5. Develop a business case for migration to include comparison of current expenditures to proposed expenditures (ranging from facility, hardware, middleware & database, infrastructure etc.), demonstrating ROI of proposed solution.
6. Provide a migration plan that describes the appropriate service models of all services to be migrated, as well as rationale for the recommended cloud models.
7. Provide recommendations for cloud migration based on applications' development lifecycle, data management, operations, business relevance, security impacts, organizational roles, financial aspects of cloud service delivery, and other migration considerations.
8. Address sourcing model that will be authorized to control where applications will be hosted based on security, performance, disaster recovery, and service level requirements.
9. Provide recommendations for incorporating government-wide and agency-specific security controls into the target design and migration plan.
10. Develop and describe approach to identify and manage communication, change management, and training needs for migration planning.
11. Develop and describe approach to ensure that procedures and documentation are developed for migration execution.
12. Develop and describe approach to cloud governance for post-implementation.
13. Deliver a technical architecture capturing the "to-be" cloud migration state that is consistent with adopted federal enterprise architecture frameworks and consistent with HHSC's architecture standards.
14. Include considerations in the migration planning solution for the target design such as capacity, schedules, migration priority, cost, etc.
15. Develop and describe approach to implement metering to migrated cloud services including provisioning capabilities, accounting capabilities, billing capabilities, etc.
16. Develop and describe approach to testing for migration planning.
17. Produce a plan that will support co-existing non-cloud and cloud architectures during and after migration.
18. Provide recommendations for a Communications Plan for all phases and affected parties of the migration to ensure end-user adoption, customer satisfaction, successful organizational process changes, and alignment with HHSC's policies, requirements and goals.

2.1.3.6. PHASE 6 – POST-MIGRATION PLANNING

1. Provide a plan for maintaining cloud services post-deployment.
2. Provide a resource management plan including resource roles, responsibilities, communication, performance, auditing, and issue resolution.
3. Maintain clear HHSC visibility into costs, schedule, technical performance, and risk, including periodic reporting.
4. Provide meaningful reporting and analytics that provide HHSC with up-to-date and comprehensive information regarding technical and management performance.
5. Prepare a legacy application and data center decommissioning timeline. During transition, legacy applications should be maintained and operational along with cloud migration solutions to support uninterrupted development of business requirements. The timeline shall conform to the business roadmaps for legacy systems and for transition to cloud-based solutions.
6. Provide Data Center decommissioning planning, including developing a multi-step decommissioning roadmap.
7. Provide planning related to data sanitization to ensure all data is destroyed, to the point of not being recoverable, on all hardware that is replaced/removed due to maintenance, upgrade, or for any other reason complying with DoD 5220.22-M or NIST SP800-88 standards.

2.1.3.7. PHASE 7– MIGRATION SUPPORT SERVICES (OPTIONAL)

HHSC may elect to exercise the optional services identified in this section. If HHSC elects to exercise these optional services, the Vendor will be required to perform them in accordance with the requirements presented in this section and to provide the associated deliverables identified in Section 2.1.5 - Deliverables.

1. Vendor will provide Application Transformation advisory and support services to assist HHSC with cloud migration plan execution.
2. Vendor will provide Cloud Security advisory and support services to assist HHSC with cloud migration plan execution.
3. Vendor will provide Cloud Migration advisory and support services to assist HHSC with cloud migration plan execution.
4. Vendor must address the Phase 7 – Migration Support Services as distinct elements in the Project Approach and Staffing Plan section of their Proposal. The Staffing Plan element must identify the proposed roles, organization, and resource FTE counts for the Phase 7 services.

5. The Migration Support Services are expected to commence within six (6) to twelve (12) months of HHSC's acceptance of the Phase 5 Cloud Migration Plan deliverable.
6. The expected duration for the Migration Support Services is minimum of six (6) months but not more than twelve (12) months.

2.1.4. DELIVERABLES

To meet the objectives of the project, the Vendor must provide deliverables as described to meet applicable business, technical, security, management, and administrative objectives. The deliverables must also align with objectives of the enterprise service delivery model, and support HHSC's ability to deliver future sustainable services.

In collaboration with HHSC, the Vendor must develop a Deliverable Expectation Document (DED) for each deliverable to clearly define the content and format for the deliverable. The DED will establish a common, agreed-upon understanding between HHSC and the Vendor regarding the purpose, scope, content, and timeline for the deliverable and will provide a process to verify the deliverable meets agreed-upon acceptance criteria. The complexity of the DED shall be proportional to the complexity of scope of the deliverable. HHSC's review, acceptance, and quality monitoring of the deliverable will be in accordance with the DED.

The Vendor must formally submit each DED to HHSC for review and approval. The Vendor must also provide a comprehensive walk-through with HHSC in advance of submittal. DEDs associated with Project Phases must be submitted within seven (7) calendar days after the scheduled start date for each Phase.

The DED for each deliverable will include the following information, at a minimum:

1. The deliverable name.
2. The deliverable purpose.
3. An outline / table of contents of the deliverable and a general description of the information will be contained in the deliverable.
4. Deliverable Acceptance Criteria which are consistent with the requirements of the SOW. Deliverable Acceptance Criteria will be initially developed by the Vendor and are subject to acceptance in writing by HHSC. If any of the Vendor's proposed criteria are unacceptable, HHSC, at its sole discretion, may set the acceptance criteria or require the Vendor to re-write and re-submit the DED for submission to and approval by HHSC within ten (10) business days after written notification of HHSC's rejection of the criteria.

The tables below summarize the deliverables that the selected Vendor will provide during the execution of the project.

Project Work Plan	
Required Delivery	Within seven (7) calendar days after the Contract Start Date.
Frequency	Subsequent submittals will be required for formal approval of changed baseline dates.
Description	• A detailed schedule in MS Project for key activities including project tasks, deliverables, and knowledge transfer activities. • A logical sequence of tasks and deliverables. • A clear narrative definition of each task and deliverable. • Staff assignments for each task and deliverable. • A specific target completion date for each task and deliverable. • Task and deliverable relationships and dependencies. • Identification of the critical path for the work plan to allow for the determination of impacts to any schedule slippage. • The Project Work Plan "actual" schedule is expected to be maintained current on at least a weekly basis. • Knowledge transfer activities and the assessment activities for readiness of the Vendor to proceed to the next project Phase.

Phase 1 – TIERS Inventory	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.1 • Detailed recommendations as required by Section 2.1.3.1

Phase 2 – TIERS Cloud Assessment	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.2 • Detailed recommendations as required by Section 2.1.3.2

Phase 3 – Application Transformation Plan	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.3 • Detailed recommendations as required by Section 2.1.3.3 • Detailed plans as required by Section 2.1.3.3

Phase 4 – Cloud Security Plan	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.4 • Detailed recommendations as required by Section 2.1.3.4 • Detailed plans as required by Section 2.1.3.4

Phase 5 – Cloud Migration Plan	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.5 • Detailed recommendations as required by Section 2.1.3.5 • Detailed plans as required by Section 2.1.3.5

Phase 6 – Post-Migration Plan	
Required Delivery	On or prior to the approved Deliverable Due Date.
Frequency	One time, dependent upon HHSC approval.
Description	• Executive summary of Phase objectives, results, and recommendations. • Detailed results as required by Section 2.1.3.6 • Detailed recommendations as required by Section 2.1.3.6 • Detailed plans as required by Section 2.1.3.6

Phase 7 – Migration Support Services Status Report (Optional)	
Required Delivery	First delivery required after first Support Services calendar month is completed.
Frequency	Monthly. The Monthly Status Report (MSR) is required to be delivered to HHSC no later than the close of business on the fifth working day of each month immediately following each reporting period.
Description	• Provide a summary of activities performed under Support Services for the reporting period. • Document all Observations, Issues, Risks, and Action Items the support services team has encountered, including associated recommendations for resolution or mitigation. • Track status of all reported Issues and Risks for Phase 7. • Report Support Services Team delivered labor hours by resource for the reporting period. • The MSR will serve as invoice backup documentation.

2.1.5. PROGRESS REPORTING

The selected Vendor will document in a Weekly Progress Report, details of project statue, schedule delays, and issues or risks impacting the project.

Weekly Status Report	
Required Delivery	First delivery required after first completed calendar week following the contract start date.
Frequency	Weekly. The Weekly Status Report is required to be delivered to HHSC no later than the close of business on the Monday immediately following each reporting period.
Description	• Weekly progress metrics • Schedule status • Noted Observations, Issues, Risks, and Action Items along with recommendations, and items that require escalation.

In addition to the Weekly Status Report, the selected Vendor will escalate any identified issues that cause, or may potentially cause, project delays to the TIERS Project Manager within 24 hours of discovery.

2.1.6. VENDOR RESPONSIBILITIES

The selected Vendor shall provide Cloud Assessment and Migration Planning Services adhering to, at a minimum, the following:

1. The selected Vendor will provide computer equipment and software for their assigned staff.

2. The selected Vendor will support a standard work week of 40 hours, Mondays through Fridays, except on closed holidays determined by the State of Texas. Normal working hours are 8:00AM to 5:00PM Central Time. Vendor staff will adjust their working/interview schedules to correspond with the working hours of the involved HHSC resources.

3. The selected Vendor's resources are expected to perform most of their services, including attending meetings, onsite at either the HHSC Centre Creek or Cross Park locations. Vendor resources should be available by phone and email during normal working hours.

4. The Vendor will designate their Project Manager and Lead Architect roles as "Key Personnel" resources.

5. The selected Vendor must provide the resume of any potential replacement resource for HHSC's review and approval prior to assigning the resource to the project. Any replacement resource must have equal or better credentials, training, and skills as the person he or she is replacing.

6. The Vendor will meet Service Level Agreements described in Section 2.1.10.

7. Vendor must complete cybersecurity training program certified under Texas Government Code, Section 2054.519, as selected by the agency. The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period.

2.1.7. HHSC RESPONSIBILITIES

1. HHSC will provide dedicated cubicle spaces for up to four (4) concurrent Vendor team members to use in a hoteling fashion when onsite at 1609 Centre Creek Drive, Austin, Texas 78754.

2. HHSC will provide all members of Vendor's team with facility parking, access to HHSC facilities to attend TIERS meetings, and access to conference rooms for the Vendor's staff.

3. HHSC will provide members of the Vendor's team with appropriate access to HHSC TIERS systems only after each resource signs and submits a Texas HHS Acceptable Use Agreement ("AUA").

4. HHSC will provide all Vendor staff with HHSC email accounts, which include appointment / meeting calendars to assist with project and assessment communications.

5. HHSC will provide a Project Manager as the customer representative for the Vendor. The HHSC Project Manager will:

    a. Coordinate with TIERS IT-SSA, TIERS DCS&O, HHSC Legal and HHSC procurement, administrative, and security staff, as needed, to resolve project and contractual issues.

    b. Receive, review, and coordinate the approval of any SOW Change Requests.

    c. In coordination with IT-SSA Director, will receive and review the Vendor Weekly Progress Reports.

    d. In coordination with IT-SSA Director, will receive, review, and approve the Vendor Deliverables.

    e. Review and approve all Vendor submitted invoices.

2.1.8. WORK PRODUCTS

The Contract awarded the Vendor will require two types of work products:

Work Artifacts: This includes all documentation produced in association with work performed against the Contract Statement of Work.

Deliverables: These artifacts are work products identified as Deliverables in the Statement of Work. These artifacts, upon acceptance by HHSC, constitute invoice and payment triggers.

All Vendor work products must be submitted to the IT-SSA Contract Manager in a format approved by HHSC, adhere to Contract terms, and be provided by the dates specified. Any changes to the delivery date must have prior written approval by HHSC. HHSC intends for work products to be published in a manner that facilitates visibility, collaboration on documents, and ease of capturing and responding to formal HHSC comments.

The Vendor must:

1. Make all work products available electronically.
2. Utilize the HHSC-provided solution for HHSC and the Vendor to propose changes to documentation work products throughout the term of the Contract.

HHSC owns all work products produced under the Contract.

HHSC will review all Deliverables and notify the Vendor in written format within ten (10) business days of its receipt of a Deliverable of its acceptance, conditional acceptance, or rejection, with the reason(s) for rejection and what the Vendor must do so that the Deliverable will be acceptable. Vendor has five (5) business days, or as otherwise agreed to by HHSC, to correct the Deliverable and resubmit it for HHSC review. HHSC will provide final acceptance of the Deliverable, at which time, the associated invoice can be submitted for payment.

While Work Artifacts under the Contract do not require a formal HHSC review and approval process, they should adhere to stated quality, content, and timeliness criteria included in this SOW.

2.1.9. INVOICING

The selected Vendor will submit an invoice to HHSC monthly. The invoice must be based on HHSC-accepted Deliverables for work completed during the preceding performance period, and on the agreed-upon price for each Deliverable as executed in the Cost Schedule.

Each invoice submitted must identify the Purchase Order number, the Contract number, and the time period (i.e., month and year) that the invoiced work was performed. Payment shall be in accordance with the Texas Prompt Payment Act, Texas Govt. Code, Section 2251.

Invoices shall be sent to:

Health and Human Services Commission
Attn: Invoice-HHSC Accounting
Health and Human Services Commission
4900 North Lamar Blvd.
Austin, TX 78751
Phone: 512-424-6518
Fax: 512-424-6901
Email: HHSC_AP@hhsc.state.tx.us

Prior to any payment being made, HHSC must certify that the services being invoiced have been received and approved by HHSC.

2.1.10. SERVICE LEVEL AGREEMENTS (SLAS)

HHSC contracts for results. A successful result may be defined as the generation of discrete, defined, measurable, and beneficial outcomes that support HHSC Statement of Work goals, service delivery agreements, and product specifications. HHSC will monitor the performance of a contract issued under this SOW. All services and work products under the Contract shall conform to this SOW at an acceptable quality level and in a manner consistent with acceptable industry standard, custom, and practice. Conformance to work product submission dates as agreed to with HHSC will be monitored. Liquidated damages for not meeting SLAs are specified in Figure 2-9.

SLA	SLA Name	Performance Evaluated	Non-Conformance	Frequency of Measurement
SLA 1	Deliverable Timeliness	100% of all Deliverables identified in Section 2.1.4 must be submitted by the date specified in the HHSC-accepted Work Plan	Liquidated Damages in the amount of $250 for each day of non-conformance, not to exceed $5,000 in any given month.	Monthly

Figure 2-9 Service Level Agreements

2.2. CONTRACT AWARD AND TERM

2.2.1. CONTRACT AWARD AND EXECUTION

HHSC intends to award one (1) fixed price deliverable Contract as a result of this Solicitation. Any award is contingent upon approval of the Executive Commissioner or their designee.

If, for any reason, a final Contract cannot be negotiated with a Respondent within ten (10) business days of HHSC's determination to seek to contract with that Respondent, HHSC may negotiate a contract with the next highest scoring Respondent or may withdraw, modify, or partially award this Solicitation.

Upon completion of the final Contract, HHSC will submit the contract to the Center for Medicare and Medicaid Studies ("CMS") and Food and Nutrition Services ("FNS") for approval. Execution of the Contract is contingent on CMS and FNS approval.

2.2.2. CONTRACT TERM

HHSC anticipates the initial duration of any Contract resulting from this SOW shall be for a period of one (1) year. HHSC, at its sole option, may extend any contract awarded pursuant to this Solicitation for up to two (2), one (1) year additional terms.

Following the base term and the allowable extension, HHSC may extend any resulting contract upon mutually agreeable terms and conditions for the purpose of maintaining needed advisory services and to avoid interruption in HHSC services.

2.3. Data Use Agreement and Security and Privacy Initial Inquiry

By entering into a Contract, or purchase order with HHSC because of this SOW, the selected Vendor agrees to be bound by the terms of the Data Use Agreement ("DUA") as well as the Security and Privacy Initial Inquiry (SPI) as referenced in **Exhibit D - Data Use Agreement and Security Privacy Initial Inquiry**. The Vendor will safeguard any confidential information to which Vendor has access in performing the services in compliance with the HHS DUA.

2.4 Insurance

By entering into a Contract, or purchase order with HHSC because of this SOW, the selected Vendor agrees to be bound by the terms of **EXHIBIT M - VENDOR INSURANCE COVERAGE**.

ARTICLE III. ADMINISTRATIVE INFORMATION

3.1. Schedule of Events

EVENT	DATE/TIME
SOW Release Date	11/22/2019
Deadline for Submitting Questions	12/5/2019 at 2:00 PM CST
Questions and Answers Posted	12/12/2019
Deadline for submission of Proposals [NOTE: Proposals must be RECEIVED by HHSC by the deadline.]	12/23/2019 at 2:00 PM CST
Anticipated Contract Start Date	4/1/2020

Note: These dates are a tentative schedule of events. HHSC reserves the right to modify these dates at any time upon notice provided to prospective Respondents. Any dates listed after the Proposal deadline will occur at the discretion of HHSC and may occur earlier or later than scheduled without notification to prospective Respondents.

3.2. Changes, Amendment or Modification to Solicitation

HHSC reserves the right to change, amend or modify any provision of this Solicitation, or to withdraw this SOW at any time prior to award if it is in the best interest of HHSC. Any such revisions are notified to prospective Respondents.

3.3. IRREGULARITIES

Any irregularities or lack of clarity in this SOW must be brought to the attention of the Point of Contact listed in Section 3.5.1 as soon as possible so corrective addenda may be furnished to prospective Respondents.

3.4. INFORMALITIES

HHSC reserves the right to waive minor informalities in a Proposal if it is in the best interest of HHSC. A "minor informality" is an omission or error that, in HHSC's determination, if waived or modified when evaluating Proposals, will not give a Respondent an unfair advantage over other Respondents or result in a material change in the Proposal or SOW requirements.

3.5. INQUIRIES

3.5.1. POINT OF CONTACT

Except as stated in sec. 3.5.3, below, all requests, questions or other communication about this SOW shall be made in writing to the HHSC's Purchasing Department, addressed to the person listed below:

Name:	Brad Westbrook
Title:	Purchaser, CTCD, CTCM
Address:	1100 W. 49th Street, Austin TX, 78756
Phone:	512-406-2557
Email:	Brad.Westbrook@hhsc.state.tx.us

All communications are strictly prohibited between Respondents and other HHSC staff members concerning this SOW. Failure to comply with these requirements may result in disqualification of Respondent's Proposal

3.5.2. QUESTIONS

HHSC will allow written questions and requests for clarification of this Solicitation. Questions must be submitted in writing and sent by U.S. First Class mail or email to the Point of Contact listed in Section 3.5.1 above. HHSC will remove Respondents' names from questions in any responses released. Questions shall be submitted in the following format. Submissions deviating from this format may not be accepted:

1. Identifying SOW number
2. Section Number
3. Paragraph Number
4. Page Number
5. Text of passage being questioned
6. Question

Note: The Point of Contact must receive questions or other written requests for clarification by the deadline set forth in Section 3.7.1 below. However, HHSC, at its sole discretion, may respond to questions or other written requests received after the deadline. Provide company name, address, phone number; fax number, e-mail address, and name of contact person when submitting questions.

3.5.3. PROHIBITED COMMUNICATION

On issuance of this Solicitation, except for the written inquiries described in Section 3.5.3 and 3.5.5 below, HHSC, its representative(s), or partners will not answer any questions or otherwise discuss the contents of this SOW with any potential Respondent or their representative(s). Attempts to ask questions by phone or in person will not be allowed or recognized as valid. Respondent shall rely only on written statements issued by or through HHSC's designated staff as provided by this Section. This restriction does not preclude discussions between affected parties for the purposes of conducting business unrelated to this Solicitation. **Failure to comply with these requirements may result in disqualification of Respondent's Proposal.**

3.5.4. CLARIFICATION

Respondents must notify the Point of Contact of any ambiguity, conflict, discrepancy, exclusionary specifications, omission or other error in the Solicitation in the manner and by the deadline for submitting questions. If a Respondent fails to properly and timely notify the Point of Contact of such issues, the Respondent submits its Proposal at its own risk. If the Respondent is awarded a Contract they: (1) shall have waived any claim of error or ambiguity in the Solicitation and any resulting Contract, (2) shall not contest the interpretation by HHSC of such provision(s), and (3) shall not be entitled to additional compensation, relief, or time by reason of ambiguity, error, or later correction.

3.5.5. RESPONSES

Responses to questions or other written requests for clarification may be provided to prospective Respondents. HHSC reserves the right to amend answers prior to the deadline for submission of Proposals. Amended answers will be provided to the prospective Respondents. HHSC also reserves the right to decline to answer any question or questions or to provide a single consolidated response of all questions they choose to answer in any manner at the HHSC's sole discretion.

3.6. PROPOSAL COMPOSITION

3.6.1. GENERAL

The Respondent shall submit a Narrative Proposal, a Required Respondent Information, and a Cost Proposal. The Respondent shall submit four (4) electronic copies of the Narrative Proposal and Required Respondent Information document in searchable portable document format (".pdf") on USB flash drives, compatible with Microsoft Office 2016. The Respondent must also submit one (1) electronic copy of the Cost Proposal on a USB flash drive.

Each copy must include all required documents. Failure to submit all required documents in required format(s) may result in disqualification of the Proposal without further consideration. A Respondent shall prepare a Proposal that clearly and concisely represents its qualifications and capabilities under this Solicitation. Expensive bindings, colored displays, promotional materials, etc. are not necessary or desired. Respondent must focus on the instructions and requirements of the Solicitation.

HHSC, in its sole discretion, may reject any and all proposals or portions thereof.

3.6.2. SUBMISSION IN SEPARATE PARTS

Proposals must be submitted in two (2) separate parts:

1. Narrative Proposal and Required Respondent Information
2. Cost Proposal

Electronic submissions must be separated by electronic medium used for submission (i.e. flash drive).

The entire Proposal must then be submitted in one package to HHSC at the address listed in Section 3.7.

3.6.3. PAGE LIMIT AND SUPPORTING DOCUMENTATION

The Narrative Proposal should not exceed thirty (30) pages in length, not including appendices or attachments, and require formatting as follows: 8 ½" x 11" paper, 12 point font size, and single-sided. Diagrams and graphs in 8 point font will be accepted. If the Respondent cannot submit complete Proposals without referencing supporting documentation, such documentation must be provided with the Proposal, with specific reference made to the tab, page, section, and/or paragraph where the supporting information can be found.

3.6.4. DISCREPANCIES

Discrepancies or disparities between the contents of original Proposals and copies will be interpreted in favor of HHSC. If the Respondent fails to designate an "ORIGINAL," HHSC may reject the Proposal or select a copy to be used as the original.

3.6.5. EXCEPTIONS

HHSC is attaching hereto as **Exhibit C - HHSC Sample Signatures Document** - that also identifies and incorporates the exhibits that will compose the HHSC proposed Contract. HHSC will more favorably evaluate Proposals that offer no or few exceptions, reservations, or limitations to the requirements, terms, and conditions of this Solicitation.

Respondents are highly encouraged, in lieu of including exceptions in their Proposals, to address all issues that might be advanced by way of exception by submitting such issues pursuant to Section 3.5.4. Any exception included in a Proposal may result in a Respondent not being awarded a Contract. If a Respondent includes exceptions in its Proposal, Respondent is required to use **Exhibit G - HHSC Exceptions and Assumptions Form.** The Vendor is required to provide all information noted on the form indicating SOW Section Number, SOW Section Title, Language to which Exception is Taken, Proposed Language, and Statement as to whether or not, by indicating "yes" or "no," if the Vendor still wants to be considered for a Contract award if the exception is denied.

Every exception must provide all required information without qualification in the format set forth in **Exhibit G - HHSC Exceptions and Assumptions Form**. Exceptions may be rejected without consideration that fail to provide all required information.

No exception, nor any other term, condition, or provision in a Proposal that differs, varies from or contradicts this SOW will be considered to be part of any Contract resulting from this SOW unless expressly made a part of the Contract in writing by HHSC.

A Proposal shall be responsive to the SOW as worded, not with any assumption that any or all terms, conditions, or provisions of the SOW will be negotiated. Furthermore, all Proposals constitute binding offers.

Note: Any Proposal to this SOW that includes any type of disclaimer or other statement indicating that the Proposal does not constitute a binding offer may be disqualified.

3.6.6. ASSUMPTIONS

Respondents must identify assumptions on **Exhibit G - HHSC Exceptions and Assumptions Form** for any business, financial, legal, programmatic, or practical assumptions that underlie the Respondent's Proposal. HHSC reserves the right to accept or reject any assumptions. All assumptions not expressly identified and incorporated into any Contract resulting from this SOW are deemed rejected by HHSC.

3.7. PROPOSAL SUBMISSION AND DELIVERY

3.7.1. DEADLINE

Proposals must be received at the address in Section 3.7.3 time-stamped by HHSC no later than the date and time specified in Section 3.1

3.7.2. LABELING

Proposals shall be placed in a sealed box and clearly labeled as follows:

Table 1- Labeling

SOW NO:	HHS0006347
SOW NAME:	TIERS Cloud Assessment and Migration Planning Services
PROPOSAL DEADLINE:	January 7, 2020 @ 2 PM CST
FOR:	TIERS Cloud Assessment and Migration Planning Services
PURCHASER NAME:	Brad Westbrook, CTCD, CTCM
RESPONDENT NAME:	

HHSC will not be held responsible for any Proposal mishandled prior to receipt by the HHSC. It is Respondent's responsibility to mark appropriately and deliver the Proposal to the HHSC by the specified date and time.

3.7.3. DELIVERY

The Respondent must deliver Proposals by one of the methods below. Proposals submitted by any other method (e.g. facsimile, telephone, email) will NOT be considered.

Table 2- Delivery Methods

U.S. Postal Service	Overnight/Express Mail	Hand Delivery
Health and Human Services Commission ATTN: Response Coordinator 1100 W. 49th St., MC 2020 Austin, Texas 78756	Health and Human Services Commission ATTN: Response Coordinator 1100 W. 49th St., MC 2020 Austin, Texas 78756	Health and Human Services Commission ATTN: Response Coordinator 1100 W. 49th St., MC 2020 Austin, Texas 78756

NOTE: All offers become the property of HHSC after submission and will not be returned to Vendor.

3.7.4. ALTERATIONS, MODIFICATIONS, AND WITHDRAWALS

Prior to the Proposal submission deadline, a Respondent may: (1) withdraw its Proposal by submitting a written request to the Point of Contact identified in Section 3.5.1; or (2) modify its Proposal by submitting a written amendment to the Point of Contact identified in Section 3.5.1. HHSC may request Proposal Modifications at any time.

ARTICLE IV. PROPOSAL EVALUATION AND AWARD PROCESS

4.1. EVALUATION CRITERIA

4.1.1. VENDOR QUALIFICATIONS

Vendor must have demonstrated experience in conducting Cloud Assessment and Migration Planning services. The selected Vendor must submit evidence of past cloud assessment projects conducted within the last five (5) years.

Proposals shall be evaluated in accordance with Title 10, Subtitle D of the Texas Government Code/ applicable law. HHSC shall not be obligated to accept the lowest priced Proposal, but shall make an award to the Respondent providing the best value to the State of Texas.

4.1.2 MINIMUM QUALIFICATIONS

Respondents must meet the minimum qualifications listed below. Furthermore, Proposals appearing unrealistic in terms of technical commitment, showing a lack of technical competence, or indicating a failure to comprehend the risk and complexity of a potential Contract may be rejected, in the sole discretion of the HHSC.

Pass/Fail Criteria

HHSC will review the following criteria on a Pass/Fail basis as follows:

1. Respondent must be authorized to do business in the State of Texas.
2. Respondent must have an active Texas franchise tax account.
3. Respondent must not be on the Texas Debarred Vendor List.
4. Respondent must not be excluded from contracting with the federal government.
5. Respondent must not be on the OIG List of Excluded Individuals and Entities.
6. Respondent must not be identified on the Texas Comptroller of Public Accounts ("CPA") Divestment Statues Lists.
7. Respondent must not have a score of D or F in the Texas CPA Vendor Performance System.

4.1.3 SPECIFIC CRITERIA

The criteria and weight to be used in determining the best value for the State of Texas is as follows:

1. Cost (30%): The reasonableness of Respondent's proposed rates and costs presented in the Cost Proposal.
2. Project Approach (30%): The Respondents proposed project approach and project work plan satisfies the Section 2.1 Description of Services/Statement of Work requirements.

3. Personnel Organization and Qualifications (20%): The Respondent's proposed staffing plan demonstrates expertise and experience necessary to support the Section 2.1 Description of Services/Statement of Work requirements.

4. Vendor Capabilities and Performance (20%): The Respondent's company information and past performance demonstrate experience with similar Cloud Assessment projects in a state or federal environment.

For a more detailed breakdown of each of the foregoing criteria, see Exhibit H - SOW HHS0006347 Proposal Evaluation Tool.

4.1.4 OTHER INFORMATION

HHSC may call/ email past performance contacts provided by a Respondent, contact Respondent's clients, or solicit information from any available source, including other departments within HHSC, other State agencies, and the CPA's Vendor Performance Tracking System.

4.2. INITIAL COMPLIANCE SCREENING

HHSC will perform an initial screening of all Proposals received. Unsigned Proposals, Proposals not meeting Section 4.1.2 above, and/or Proposals that do not include all required forms and information may be subject to rejection without further evaluation.

4.3. COMPETITIVE RANGE AND BEST AND FINAL OFFER

HHSC may determine certain Proposals are within the competitive range and may use this as a basis to request a Best and Final Offer ("BAFO") from Respondents. If HHSC elects to limit award consideration to a competitive range, the competitive range will consist of the Proposals that receive the highest or most satisfactory ratings based on the published evaluation criteria and procedures governing this procurement. HHSC, in the interest of administrative efficiency, may place reasonable limits on the number of Proposals included in the competitive range.

HHSC may, at its discretion, request all Respondents provide a BAFO. A request for a BAFO from HHSC does not guarantee an award or further negotiations.

4.4. ORAL PRESENTATIONS AND SITE VISITS

HHSC may require an oral presentation from any or all Respondents. Respondents will be provided with advance notice of any such oral presentation and are responsible for their own presentation equipment. Failure to participate in the requested presentation may eliminate a Respondent from further consideration. HHSC is not responsible for any costs incurred by the Respondent in preparation for any oral presentation.

4.5. QUESTIONS OR REQUESTS FOR CLARIFICATION BY THE HHSC

HHSC reserves the right to ask questions or request clarification from any Respondent at any time during the SOW process, including during Oral Presentations, Site Visits, or during the BAFO process.

ARTICLE V. NARRATIVE PROPOSAL

The Narrative Proposal shall contain the following information below.

5.1. EXECUTIVE SUMMARY

Respondent must provide an Executive Summary of the proposal (excluding any cost information) asserting the approach and qualifications for meeting the SOW requirements. The summary must demonstrate an understanding of HHSC's goals and objectives for the Solicitation. The Executive Summary must not exceed five pages and must represent a full and concise summary of the contents of the proposal**. Vendor must identify its specific DIR contract by DIR number.**

5.2. PROJECT APPROACH

Describe the Respondent's proposed strategies, processes, and methodologies for providing all phases of the Scope of Work described in Section 2.1.3. At a minimum, the project approach should address the following items:

1. Describe approach and methodology for identifying the business processes and governance processes that are associated with current applications and infrastructure inventory.
2. Describe approach for inventorying the infrastructure such as hardware, application, middleware & databases, networks, as well as any other relevant factors or components of the infrastructure.
3. Describe approach to developing application evaluation, profiling, and dependency mapping criteria.
4. Describe approach to developing a business case for migration to include comparison of current expenditures to proposed expenditures (ranging from facility, hardware, middleware & database, infrastructure etc.), demonstrating ROI of proposed solution.
5. Describe approach to cloud security planning throughout this assessment and advise on the approach to such planning for future implementation.
6. Describe approach to providing technical advice to cloud migration that will enable HHSC to implement metering to migrated cloud services including provisioning capabilities, accounting capabilities, billing capabilities, etc.
7. Describe approach to testing for migration planning.
8. Describe tools and analysis techniques to be used for analyzing, evaluating, and presenting information gathered throughout the migration planning phases. Identify or provide examples of the proposed tools. Describe methodology for utilization of auto-discovery tools to complete the inventory tasks.

5.3. Staffing Plan

Respondent must provide a staffing plan that identifies all resources that will be responsible for the performance of the services requested under this Solicitation. The staffing plan must describe the project organization, number of resources to be provided, each member's skillset and/or qualifications, and how the Respondent plans to remediate planned or unplanned changes in personnel during the project.

Respondent must provide resumes for all staff identified in the staffing plan. The resource expertise and experience should be aligned with the services described in Article II. Each resume must include:

1. Professional employment history, with dates
2. Education (degrees received and major studies)
3. Knowledge of and expertise with the subject matter of this SOW
4. Relevant experience in projects similar to the scope of this SOW
5. Relevant state and/or federal government experience
6. Past performance roles and responsibilities
7. Professional certifications

HHSC expects that the staff specified in a Respondent's Proposal be the persons that are provided to perform the services of this SOW. In the case of the role defined as Key Personnel, HHSC requires the proposed individual be provided on the project team.

5.4. Project Work Plan

Respondent must provide a proposed Project Work Plan that identifies the recommended tasks, timeline, and scheduled Deliverable due dates for the project. The requirements for this plan are presented in Section 2.1.4.

5.5. Example Work Products

Respondent must provide examples of work products that demonstrate their expertise and experience with the services required by this SOW. The table below presents the preferred types of work products for these examples. If available, Respondent should provide examples completed for states of comparable size or federal agencies.

Work Product	Description
Risk Assessment	Risks and mitigations associated with moving applications and data to the cloud.
Business Case	Cost and benefits of migrating from an in-house data center to a cloud environment.
Cloud Requirements	Technical requirements for moving applications and data from an in-house data center to a cloud environment.
Project Schedule	Work breakdown structure of work to be performed, which resources of the organization will perform the work and the timeframes in which that work needs to be performed.
Application Assessment	Assessment of methodologies required to move applications and/or data sets to the cloud.

Work Product	Description
Cloud Solution Assessment	Comparison showing how cloud service providers' solutions are assessed and selected.
Application Transformation	Assessment of approaches for moving applications to the cloud, including analysis of storage, memory, processor, and network requirements.
Cloud Migration Recommendations	Overall recommendations and strategies for migrating to the cloud.
Cloud Migration Roadmap	Objectives, approach, activities, and timeline to get from an in-house data center to the cloud.

ARTICLE VI. REQUIRED RESPONDENT INFORMATION

6.1. COMPANY INFORMATION

Respondent must provide satisfactory evidence of its ability to manage and coordinate the types of activities described in this SOW and to produce the specified goods or services on time. As a part of the Proposal requested in Article III, Respondent must provide the information below.

6.1.1. COMPANY NARRATIVE

Provide a detailed narrative explaining why Respondent is qualified to provide the services enumerated in Article II, focusing on its company's key strengths and competitive advantages.

6.1.2. COMPANY PROFILE

Using **Exhibit L - Vendor Information and Disclosures** as a template for completion, the Respondent must provide a company profile.

Note: If the Respondent is an out-of-state company, a Certificate of Authority from the Secretary of State to do business in Texas must be provided as well.

6.2. PAST PERFORMANCE

Using **Exhibit K – Past Performance Template** as a template for completion, the Respondent shall list and provide information concerning a minimum of three (3) contracts or projects similar to the services enumerated in Article II. HHSC prefers information from projects or contracts that were performed for states of comparable size and/or federal government within the last five (5) years. Respondents must verify client contacts are current.

6.3. MAJOR SUBCONTRACTOR INFORMATION

Respondent must identify any major subcontractors whom Respondent intends to utilize in performing fifteen percent (15%) or more of the work on the Contract. The Respondent must indicate whether or not Respondent holds any financial interest in any major subcontractor. It may be required as a condition of award that an authorized officer or agent of each proposed major subcontractor sign a statement to the effect that the subcontractor has read, and will agree to abide by, Respondent's obligations under any contract awarded pursuant to this Solicitation.

6.4. LITIGATION AND CONTRACT HISTORY

Respondent must include in its Proposal a complete disclosure of any alleged or significant contractual failures. In addition, Respondent must disclose any civil or criminal litigations or investigations over the last five (5) years that involves Respondent or in which Respondent has been judged guilty or liable including any allegations of such that are currently pending.

Respondent must also disclose any settlement agreements executed in the last five (5) years related to alleged contractual failures. Failure to comply with the terms of this provision

may disqualify Respondent. A Proposal may be rejected based upon Respondent's prior history with the State of Texas or with any other party that demonstrates, without limitation, unsatisfactory performance, adversarial or contentious demeanor, or significant failure(s) to meet contractual obligations.

6.5. Conflicts of Interest

Respondent must certify it does not have any personal or business interests that present a conflict of interest with respect to the SOW and any resulting Contract. Additionally, if applicable, the Respondent must disclose all potential conflicts of interest. The Respondent must describe the measures it will take to ensure there will be no actual conflict of interest and that its fairness, independence and objectivity will be maintained. HHSC will determine to what extent, if any, a potential conflict of interest can be mitigated and managed during the term of the Contract. Failure to identify actual and potential conflicts of interest may result in disqualification of a Proposal or termination of a Contract.

Include any activities of affiliated or parent organizations and individuals who may be assigned to this Contract, if any.

Additionally, pursuant to Section 2252.908 of the Texas Government Code, a successful Respondent awarded a Contract greater than $1 million dollars, or that requires an action or vote of the governing body, must submit a disclosure of interested parties to HHSC at the time the business entity submits the signed Contract. Rules and filing instructions may be found on the Texas Ethics Commission's public website and additional instructions will be given by HHSC to successful Respondents.

6.6. Affirmations and Certifications

Respondent must complete and return the following listed forms:

1. Exhibit B – HHSC Affirmations and Solicitation Acceptance
2. Exhibit D – Data Use Agreement (DUA) and Security and Privacy Initial Inquiry (SPI)
3. Exhibit E – Lobbying Certification
4. Exhibit E1 – Federal Assurances -Non-Construction
5. Exhibit F – Fiscal Federal Funding Accountability and Transparency Act ("FFATA") Certification
6. Exhibit G – HHSC Exceptions and Assumptions Form (if applicable)

6.7. Financial Security

Respondents with a Dun and Bradstreet number must include a Comprehensive Insight Plus Report, Business Information Report or Credit eValuator Report with their Solicitation Response.

6.8. HUB SUBCONTRACTING PLAN

HHS will require the Respondent to comply with their current HUB Subcontracting Plan with DIR for any contract executed as a result of this solicitation.

ARTICLE VII. COST PROPOSAL

7.1. COST PROPOSAL

As noted in Section 3.6, cost information must not be included with the Narrative Proposal or the Required Respondent Information. Respondent must submit a Cost Proposal for the services listed in Article II, Statement of Work, by completing the **Exhibit I - Services Rate Schedule** and the **Exhibit J - Deliverable Cost Schedule**. Except for hardware, software, tools, supplies and other personnel or support to be provided by HHSC under Section 2.1.7, all Respondent costs must be included in the Deliverable Cost Schedule and Services Rate Schedule.

The Cost Proposal should corroborate the Respondent's response to the Narrative Proposal and describe how the Respondent plans to complete the work requested. Respondent's Cost Proposal will include all of the total planned costs for the Term of the Contract. Recall that the Term is one (1) year for the services.

For the Deliverable Cost Schedule, Respondent must provide Deliverable pricing for the proposed project team that would support activities as defined in Section 2.1.3. Respondent's Services Rate Schedule must, where applicable, conform to the current Category and Level identified with the Texas Department of Information Resources ("DIR"), IT Services Contract ("ITSAC"), Not-To-Exceed Pricing Final document for similar or substantially similar services. It can be found here: http://dir.texas.gov/ using the search feature for "ITSAC Not to Exceed."

The Cost Proposal must include any business, economic, legal, programmatic, or practical assumptions that underlie the Respondent's proposed costs. The assumptions must be described in a separate Exhibit G - Exceptions and Assumptions form that is included in the Cost Proposal. HHSC reserves the right to accept or reject any exceptions or assumptions. All exceptions and assumptions not expressly identified and incorporated into the contract resulting from this SOW are deemed rejected by HHSC.

Respondent must submit the Cost Proposal response in a separate, sealed package, labeled as per Section 3.7.2, and additionally labeled, "Cost Proposal."

ARTICLE VIII. GENERAL INFORMATION

8.1. General Information

8.1.1. Amendment

HHSC reserves the right to alter, amend or modify any provision of this SOW, or to withdraw this Solicitation, at any time prior to award, if it is in the best interest of the State.

8.1.2. Offer Period

Proposals shall be binding for a period of ninety (90) business days after the due date for submission of Proposals. Each Respondent may extend the time for which its Proposal will be honored. Upon Contract execution, prices agreed upon by the Respondent(s) are an irrevocable offer for the term of the Contract and any Contract renewals or extension(s). No other costs, rates, or fees shall be payable to the Respondent unless expressly agreed upon in writing by HHSC.

8.1.3. Costs Incurred

Respondents understand that issuance of this SOW in no way constitutes a commitment by HHSC to award a Contract or to pay any costs incurred by a Respondent in the preparation of a Proposal. HHSC is not liable for any costs incurred by a Respondent prior to issuance of or entering into a formal agreement, Contract, or purchase order. Costs of developing Proposals, preparing for or participating in oral presentations and site visits, or any other similar expenses incurred by a Respondent are entirely the responsibility of the Respondent, and will not be reimbursed in any manner by the State of Texas.

8.1.4. Contract Responsibility

HHSC will look solely to the selected Vendor for performance of all contractual obligations that may result from an award based on this SOW. The selected Vendor shall not be relieved of its obligations for any nonperformance by its subcontractors.

8.1.5. Public Information Act

Offers are subject to the Texas Public Information Act (PIA), Texas Government Code Chapter 552, and may be disclosed to the public upon request. Subject to the PIA, certain information may be protected from public release. Vendors who wish to protect portions of the offer from public disclosure should familiarize themselves with this law. Information pertaining to the offer will be withheld or released only in accordance with the PIA. In its offer Vendor must clearly mark any information it claims is confidential information and provide written notice to HHSC that it considers the marked information confidential. Any page in the offer submitted containing confidential information must be clearly marked with word “CONFIDENTIAL” in 14-point, red font either on top or bottom of the page. In addition, Vendors must highlight or otherwise clearly mark the specific information it considers excepted from disclosure under the PIA. HHSC will notify Vendor of any request for information that includes material Vendor identified as confidential, or otherwise excepted from disclosure. Vendor is required to demonstrate to the Office of Attorney General of Texas the specific reasons why the requested information is confidential or otherwise excepted from required public disclosure under law. Vendor will provide HHSC with copies of all such communications.

8.2. PROTEST

If a Respondent wishes to file a protest they may do so in accordance with the rules published by HHSC in the Texas Administrative Code.

ARTICLE IX. SUBMISSION CHECKLIST

This checklist is provided for Respondent's convenience only and identifies documents requested in this Solicitation.

Original Proposal Package

The "Original" Proposal must be submitted in hard copy consisting of two parts described in detail below, each under separate cover but packaged together and clearly labeled "Original" on each.

1. Narrative Proposal and Required Respondent Information

Please structure proposal responses based on the letter sequence below.

a.	Narrative Proposal	(Section 5.1 to 5.5)	____
b.	Company Information	(Section 6.1)	____
c.	Past Performance	(Section 6.2)	____
d.	Major Subcontractor Information	(Section 6.3)	____
e.	Litigation and Contract History	(Section 6.4)	____
f.	Conflicts	(Section 6.5)	____
g.	Affirmations and Certifications	(Section 6.6)	____
h.	Exceptions and Assumptions	(Sections 3.6.5 and 3.6.6)	____
i.	Staff Resumes	(Section 5.3)	____
j.	Example Work Products	(Section 5.6)	____
k.	Financial Report	(Section 6.7)	____

Appendices for Narrative Proposal and Required Respondent Information

a. Exhibit B – HHSC Affirmations and Solicitation Acceptance
b. Exhibit D – Data Use Agreement (DUA) and Security and Privacy Initial Inquiry (SPI)
c. Exhibit E – Lobbying Certification
d. Exhibit E1 – Federal Assurances -Non-Construction
e. Exhibit F – Fiscal Federal Funding Accountability and Transparency Act ("FFATA") Certification
f. Exhibit G – HHSC Exceptions and Assumptions Form (if applicable)
g. Exhibit K – Past Performance Template
h. Exhibit L – Vendor Information and Disclosures

2. **Cost Proposal**

   a. Narrative Article (7.1) ____

   b. Exhibit I - Services Rate Schedule ____

   c. Exhibit J - Deliverable Cost Schedule ____

Copies to be Provided

Copies to be provided (all clearly labeled as "Copy")	
Description	**Checkbox**
__4__ Electronic copies f **Narrative Proposal and Required Respondent Information** in **searchable** PDF on individual USB Drives.	☐
__1__ Electronic copy of **Cost Proposal** in on a USB Drive.	☐

ARTICLE X: EXHIBITS AND ATTACHMENTS

EXHIBIT A (TO BE ATTACHED) – VENDOR'S DIR DBITS CONTRACT, INCLUDING EXHIBIT A THERETO - STANDARD TERMS AND CONDITIONS

EXHIBIT B – HHSC AFFIRMATIONS AND SOLICITATION ACCEPTANCE

EXHIBIT C – SAMPLE SIGNATURES DOCUMENT

EXHIBIT C1 – HHSC UNIFORM TERMS AND CONDITIONS

EXHIBIT C2 – HHSC SPECIAL CONDITIONS

EXHIBIT D – HHSC DATA USE AGREEMENT (DUA) AND SECURITY AND PRIVACY INITIAL INQUIRY (SPI)

EXHIBIT E – LOBBYING CERTIFICATION

EXHIBIT E1 – FEDERAL ASSURANCES - NON-CONSTRUCTION

EXHIBIT F – FFATA CERTIFICATION

EXHIBIT G – HHSC EXCEPTIONS AND ASSUMPTIONS FORM

EXHIBIT H – SOW HHS0006347 PROPOSAL EVALUATION TOOL

EXHIBIT I - SERVICES RATE SCHEDULE

EXHIBIT J– DELIVERABLE COST SCHEDULE

EXHIBIT K – PAST PERFORMANCE TEMPLATE

EXHIBIT L – VENDOR INFORMATION AND DISCLOSURES

EXHIBIT M - VENDOR INSURANCE COVERAGE

THE FOLLOWING ATTACHMENTS ARE FOR REFERENCE ONLY:

ATTACHMENT A – HHSC AND TIERS BACKGROUND INFORMATION

ATTACHMENT B – TIERS AND EST APPLICATIONS OVERVIEW

ATTACHMENT C – TIERS FUNCTIONAL AND ARCHITECTURE OVERVIEW

ATTACHMENT D – TIERS CONFIGURATION MANAGEMENT PLAN V4.0

ATTACHMENT E – TIERS DCS IS CONTROLS

ATTACHMENT F – HHS INFORMATION SECURITY (IS CONTROLS) V1.0

ATTACHMENT G - INFORMATION SECURITY ASSESSMENT SUPPLEMENTAL GUIDANCE FOR EXTERNAL ENTITIES

Exhibit B: HHSC Affirmations and Solicitation Acceptance

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Exhibit B. HHSC AFFIRMATIONS AND SOLICITATION ACCEPTANCE

In this document, the terms Respondent, Contractor, Applicant, and Vendor, when referring to certifications, representations, or warranties, refer to Respondent.

Respondent affirms, without exception, as follows:

1. Respondent represents and warrants that all certifications, representations, warranties, and other provisions in this Affirmations and Solicitation Acceptance apply to Respondent and all of Respondent's principals, officers, directors, shareholders, partners, owners, agents, employees, subcontractors, independent contractors, and any other representatives who may provide services under, who have a financial interest in, or otherwise are interested in this Solicitation or any contract resulting from this Solicitation.
2. Respondent represents and warrants that all statements and information provided to HHSC are current, complete, and accurate. This includes all statements and information in this Solicitation Response.
3. Respondent understands that HHSC will comply with the Texas Public Information Act (Chapter 552 of the Texas Government Code) as interpreted by judicial rulings and opinions of the Attorney General of the State of Texas. Information, documentation, and other material prepared and submitted in connection with this Solicitation or any resulting contract may be subject to public disclosure pursuant to the Texas Public Information Act. In accordance with Section 2252.907 of the Texas Government Code, Respondent is required to make any information created or exchanged with the State pursuant to the contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.
4. Respondent acknowledges its obligation to specifically identify information it contends to be confidential or proprietary and, if Respondent designated substantial portions of its Solicitation Response or its entire Solicitation Response as confidential or proprietary, the Solicitation Response is subject to being disqualified.
5. Respondent's Solicitation Response will remain a firm and binding offer for 365 days from the date the Solicitation Response is due.
6. Respondent accepts the Solicitation terms and conditions unless specifically noted by exceptions advanced in the form and manner directed in the Solicitation. Respondent agrees that all exceptions to the Solicitation are rejected unless expressly accepted by HHSC.
7. Respondent agrees that HHSC has the right to use, produce, and distribute copies of and to disclose to HHSC employees, agents, and contractors and other governmental entities

all or part of Respondent's Solicitation Response as HHSC deems necessary to complete the procurement process or comply with state or federal laws.

8. Respondent generally releases from liability and waives all claims against any party providing information about the Respondent at the request of HHSC.

9. Respondent acknowledges all addenda and amendments to the Solicitation.

10. Respondent certifies that if a Texas address is shown as the address of Respondent on this Response, Respondent qualifies as a Texas Bidder as defined in Section 2155.444(c) of the Texas Government Code.

11. Respondent represents and warrants that it qualifies for all preferences claimed under 34 Texas Administrative Code, Section 20.306 or Chapter 2155, Subchapter H of the Texas Government Code as indicated below (check applicable boxes):

    a. Goods produced or offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
    b. Goods produced in Texas or offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
    c. Agricultural products grown in Texas
    d. Agricultural products offered by a Texas bidder
    e. Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
    f. Services offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
    g. Texas Vegetation Native to the Region
    h. USA-produced supplies, materials or equipment
    i. Products of persons with mental or physical disabilities
    j. Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel
    k. Energy efficient products
    l. Rubberized asphalt paving material
    m. Recycled motor oil and lubricants
    n. Products produced at facilities located on formerly contaminated property
    o. Products and services from economically depressed or blighted areas
    p. Vendors that meet or exceed air quality standards
    q. Recycled or reused computer equipment of other manufacturers
    r. Foods of higher nutritional value
    s. Commercial production company or advertising agency located in Texas

12. Respondent has not given, has not offered to give, and does not intend to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with this Solicitation Response, this Solicitation, or any contract resulting from this Solicitation.

13. Under Section 2155.004, Texas Government Code (relating to financial participation in preparing solicitations), Respondent certifies that the individual or business entity named in this Response or contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate.

14. Under Sections 2155.006 and 2261.053 of the Texas Government Code (relating to convictions and penalties regarding Hurricane Rita, Hurricane Katrina, and other disasters), the Respondent certifies that the individual or business entity named in this bid or contract is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate.

15. Under Section 231.006(d) of the Texas Family Code regarding child support, Respondent certifies that the individual or business entity named in this Response is not ineligible to receive the specified payment and acknowledges that the contract may be terminated and payment may be withheld if this certification is inaccurate. Furthermore, any Respondent subject to Section 231.006 of the Texas Family Code must include in the Response the names and social security numbers (SSNs) of each person with at least 25% ownership of the business entity submitting the Response:

    Name: _____ SSN: _____

    Name: _____ SSN: _____

    Name: _____ SSN: _____

    Name: _____ SSN: _____

    FEDERAL PRIVACY ACT NOTICE: This notice is given pursuant to the Federal Privacy Act. Disclosure of requested SSNs is required under Section 231.006(c) and Section 231.302(c)(2), Texas Family Code. The SSNs will be used to identify persons that may owe child support. The SSNs will be kept confidential to the fullest extent permitted by law.

    If submitted by email, Responses containing SSNs must be encrypted. Failure by a Respondent to provide or encrypt the SSNs as required may result in disqualification of the Respondent's Response.

16. Respondent certifies that it and its principals are not suspended or debarred from doing business with the state or federal government as listed on the *State of Texas Debarred Vendor List* maintained by the Texas Comptroller of Public Accounts and the *System for Award Management (SAM*) maintained by the General Services Administration. This certification is made pursuant to the regulations implementing Executive Order 12549 and Executive Order 12689, Debarment and Suspension, 2 C.F.R. Part 376, and any relevant regulations promulgated by the Department or Agency funding this project. This provision shall be included in its entirety in Respondent’s subcontracts, if any, if payment in whole or in part is from federal funds.

17. Respondent certifies that it is not listed on the federal government's terrorism watch list as described in Executive Order 13224.

18. Respondent represents and warrants that it is not engaged in business with Iran, Sudan, or a foreign terrorist organization, as prohibited by Section 2252.152 of the Texas Government Code.

19. In accordance with Section 669.003 of the Texas Government Code, relating to contracting with the executive head of a state agency, Respondent certifies that it is not (1) the executive head of an HHS agency, (2) a person who at any time during the four years before the date of the contract was the executive head of an HHS agency, or (3) a person who employs a current or former executive head of an HHS agency.

20. Respondent represents and warrants that it is not currently delinquent in the payment of any franchise taxes owed the State of Texas under Chapter 171 of the Texas Tax Code.

21. Respondent agrees that any payments due under any contract resulting from this Solicitation shall be applied towards any debt or delinquency that is owed to the State of Texas.

22. Respondent represents and warrants that payments to Respondent and Respondent's receipt of appropriated or other funds under any contract resulting from this Solicitation are not prohibited by Sections 556.005, 556.0055, or 556.008 of the Texas Government Code (relating to use of appropriated money or state funds to employ or pay lobbyists, lobbying expenses, or influence legislation).

23. Respondent agrees to comply with Section 2155.4441 of the Texas Government Code, requiring the purchase of products and materials produced in the State of Texas in performing service contracts.

24. Respondent agrees that upon request of HHSC, Respondent shall provide copies of its most recent business continuity and disaster recovery plans.

25. Respondent expressly acknowledges that state funds may not be expended in connection with the purchase of an automated information system unless that system meets certain statutory requirements relating to accessibility by persons with visual impairments. Accordingly, Respondent represents and warrants to HHSC that the technology provided to HHSC for purchase is capable, either by virtue of features included within the technology or because it is readily adaptable by use with other technology, of:
    a. providing equivalent access for effective use by both visual and non-visual means;
    b. presenting information, including prompts used for interactive communications, in formats intended for non-visual use; and
    c. being integrated into networks for obtaining, retrieving, and disseminating information used by individuals who are not blind or visually impaired.

    For purposes of this Section, the phrase "equivalent access" means a substantially similar ability to communicate with or make use of the technology, either directly by features incorporated within the technology or by other reasonable means such as assistive devices or services which would constitute reasonable accommodations under the

Americans With Disabilities Act or similar state or federal laws. Examples of methods by which equivalent access may be provided include, but are not limited to, keyboard alternatives to mouse commands and other means of navigating graphical displays, and customizable display appearance.

In accordance with Section 2157.005 of the Texas Government Code, the Technology Access Clause contract provision remains in effect for any contract entered into before September 1, 2006.

26. If Respondent is submitting a Response for the purchase or lease of computer equipment, then Respondent certifies that it is in compliance with Subchapter Y, Chapter 361 of the Texas Health and Safety Code related to the Computer Equipment Recycling Program and the Texas Commission on Environmental Quality rules in 30 TAC Chapter 328.
27. If Respondent is submitting a Response for the purchase or lease of covered television equipment, then Respondent certifies that it is compliance with Subchapter Z, Chapter 361 of the Texas Health and Safety Code related to the Television Equipment Recycling Program.
28. Should Respondent be awarded a contract resulting from this solicitation, Respondent represents and warrants, during the twelve (12) month period immediately prior to the date of the execution of the contract, none of its employees including, but not limited to those will provide services under the contract, were employees of an HHS Agency.
29. Respondent acknowledges that, pursuant to Section 572.069 of the Texas Government Code, a former state officer or employee of a state agency who during the period of state service or employment participated on behalf of a state agency in a procurement or contract negotiation involving Respondent may not accept employment from Respondent before the second anniversary of the date the contract is signed or the procurement is terminated or withdrawn.
30. Respondent represents and warrants that it has no actual or potential conflicts of interest in providing the requested goods or services to HHSC under this Solicitation and any resulting contract and that Respondent’s provision of the requested goods and/or services under this Solicitation and any resulting contract will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.
31. Respondent understands that HHSC does not tolerate any type of fraud. The agency's policy is to promote consistent, legal, and ethical organizational behavior by assigning responsibilities and providing guidelines to enforce controls. Violations of law, agency policies, or standards of ethical conduct will be investigated, and appropriate actions will be taken. All employees or contractors who suspect fraud, waste or abuse (including employee misconduct that would constitute fraud, waste, or abuse) are required to immediately report the questionable activity to both the Health and Human Services Commission's Office of the Inspector General at 1-800-436-6184 and the State Auditor's Office. Respondent agrees to comply with all applicable laws, rules, regulations, and HHSC policies regarding fraud including, but not limited to, HHS Circular C-027.

32. The undersigned affirms under penalty of perjury of the laws of the State of Texas that (a) in connection with this Response, neither I nor any representative of the Respondent has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15; (b) in connection with this Response, neither I nor any representative of the Respondent has violated any federal antitrust law; and (c) neither I nor any representative of the Respondent has directly or indirectly communicated any of the contents of this Response to a competitor of the Respondent or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Respondent.

33. Respondent represents and warrants that it is not aware of and has received no notice of any court or governmental agency proceeding, investigation, or other action pending or threatened against Respondent or any of the individuals or entities included in numbered paragraph 1 of this Affirmations and Solicitation Acceptance within the five (5) calendar years immediately preceding the submission of this Solicitation response that would or could impair Respondent's performance under any contract resulting from this Solicitation, relate to the contracted or similar goods or services, or otherwise be relevant to HHSC's consideration of entering into a contract. If Respondent is unable to make the preceding representation and warranty, then Respondent instead represents and warrants that it has provided to HHSC a complete, detailed disclosure of any such court or governmental agency proceeding, investigation, or other action that would or could impair Respondent's performance under a contract awarded as a result of this Solicitation, relate to the contracted or similar goods or services, or otherwise be relevant to HHSC's consideration of entering into a contract. In addition, Respondent acknowledges this is a continuing disclosure requirement. Respondent represents and warrants that, if awarded a contract as a result of this Solicitation, Respondent shall notify HHSC in writing within five (5) business days of any changes to the representations or warranties in this clause and understands that failure to so timely update HHSC shall constitute breach of contract and may result in immediate contract termination.

34. Pursuant to Section 2270.002 of the Texas Government Code, Respondent certifies that either (i) it meets an exemption criteria under Section 2270.002; or (ii) it does not boycott Israel and will not boycott Israel during the term of the contract resulting from this Solicitation. Respondent shall state any facts that make it exempt from the boycott certification in its Solicitation Response.

35. Respondent certifies that for contracts for services, Respondent shall utilize the U.S. Department of Homeland Security's E-Verify system during the term of the contract to determine the eligibility of:

    (a) all persons employed by Respondent to perform duties within Texas; and

    (b) all persons, including subcontractors, assigned by Respondent to perform work pursuant to the contract within the United States of America.

36. Respondent understands, acknowledges, and agrees that any false representation or any failure to comply with a representation, warranty, or certification made by Respondent is

subject to all civil and criminal consequences provided at law or in equity including, but not limited to, immediate termination of any contract resulting from this Solicitation.

37. Respondent represents and warrants that it will comply with all applicable laws and maintain all permits and licenses required by applicable city, county, state, and federal rules, regulations, statutes, codes, and other laws that pertain to any contract resulting from this Solicitation.

38. Respondent represents and warrants that all statements and information prepared and submitted in this document are current, complete, true, and accurate. Submitting a Response with a false statement or material misrepresentations made during the performance of a contract is a material breach of contract and may void the submitted Response and any resulting contract.

39. By submitting this Response, Respondent represents and warrants that the individual submitting this document and the documents made part of this Response is authorized to sign such documents on behalf of the Respondent and to bind the Respondent under any contract that may result from the submission of this Response.

Authorized representative on behalf of Respondent must complete and sign the following:

Legal Name of Respondent: _____

Signature of Authorized Representative	**Date Signed**
Printed Name and Title of Authorized Representative	**Phone Number**
Federal Employer Identification Number	**Fax Number**
DUNS Number	**Email Address**
Physical Street Address	**City, State, Zip Code**
Mailing Address, if different	**City, State, Zip Code**

Exhibit C: HHSC Sample Signatures Document

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment Planning and Migration Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

SIGNATURE DOCUMENT FOR
HHSC CONTRACT NO. _____

I. PURPOSE

The Health and Human Services Commission ("HHSC"), an administrative agency within the executive department of the State of Texas and having its principal office at 4900 N. Lamar Blvd., Austin, TX 78756. and _____ ("Contractor"), having its principal office at _____ (each a "Party" and collectively "the Parties") enter into the following contract for Cloud Assessment, Planning and Migration Services (the "Contract").

II. LEGAL AUTHORITY

This Contract is authorized by and in compliance with the provisions of Title 10, Subtitle D of the Texas Government Code (TAC), in particular Texas Government Code, §2155.144 and §2157.068

III. STATEMENT OF SERVICES TO BE PROVIDED/ORDER OF PRECEDENCE

Contractor shall perform or cause to be performed the Services in accordance with the **Statement of Work**, Services Rate Schedule and Deliverable Cost Schedule, attached hereto and incorporated herein as **Exhibits A through C**, respectively. The terms and conditions of this Contract may not weaken or diminish any terms and conditions in the DIR Contract; to the extent that the DIR Contract provides more favorable terms to HHSC or imposes more rigorous obligations on Contractor, the DIR Contract supersedes and controls over the Contract; for any other conflict between the terms and conditions of the Contract and the terms and conditions of the DIR Contract, the Contract supersedes and controls over the DIR Contract.

IV. DURATION

The Contract is effective on the signature date of the latter of the Parties to sign this agreement and terminates on _____, unless renewed, extended, or terminated pursuant to the terms and conditions of the Contract. HHSC, at its own discretion, may extend this Contract for (2), two (2) year extensions, subject to terms and conditions mutually agreeable to the Parties.

V. BUDGET

The total amount of this Contract will not exceed **[TOTAL CONTRACT AMOUNT ($ 00.00)]**. All expenditures under the Contract will be in accordance with **the DELIVERABLE COST SCHEDULE**.

VI. CONTRACT REPRESENTATIVES

The following will act as the Representative authorized to administer activities under this Contract on behalf of their respective Party.

HHSC
Health and Human Services Commission
4900 N. Lamar Blvd
Austin, TX 78751
Attention:

Contractor
Contractor Name
Address
City, State ZIP
Attention: *

VII. LEGAL NOTICES

Any legal notice required under this Contract shall be deemed delivered when deposited by HHSC either in the United States mail, postage paid, certified, return receipt requested; or with a common carrier, overnight, signature required, to the appropriate address below:

HHSC
Health and Human Services Commission
4900 N. Lamar Blvd
Austin, TX 78751
Attention: Dr. Courtney N. Phillips

With a copy to:
Health and Human Services Commission
4900 N. Lamar Blvd
Austin, TX 78751
Attention: Karen Ray, Chief Counsel

Contractor
Contractor Name
Address
City, State ZIP
Attention: *

Legal notice given by Contractor shall be deemed effective when received by HHSC. Either Party may change its address for notice by written notice to the other Party.

VIII. INSURANCE

Article VIII, section 8.2 of the HHSC Uniform Terms and Conditions, Insurance, is hereby deleted and replaced with the following Language:

1. As specified in attached **Vendor Insurance Coverage**, Contractor will acquire and maintain for the duration of this Contract, the insurance coverage required therein to ensure proper fulfillment of this Contract and protect against potential liabilities thereunder. Coverage shall be written on an occurrence basis by companies authorized and admitted to do business in the State of Texas and rated A or better by A.M. Best Company or similar rating company or otherwise acceptable to Owner.

2. The insurance shall be evidenced by delivery to Owner of certificates of insurance executed by the insurer or its authorized agent stating coverages, limits, expiration dates and compliance with all applicable required provisions. Upon request, Owner, and/or its agents, shall be entitled to receive without expense, copies of the policies and all endorsements. Neither a failure by HHSC to demand such certificates or other evidence of Contractor's full compliance with these insurance requirements nor any failure of HHSC to identify a deficiency in compliance from the evidence provided shall not be construed as a waiver of Contractor's obligation to maintain such insurance.

3. Contractor shall update all expired policies prior to submission for monthly payment. Failure to update policies shall be reason for withholding of payment until renewal is provided to Owner. Failure to maintain insurance coverage, as required, is grounds for suspension of the Work by HHSC without liability to the Contractor.

4. The insurance and insurance limits required herein shall not be deemed as a limitation on Contractor’s liability under the indemnities granted to Owner in the Contract Documents. The insurance coverage and limits established herein shall not be interpreted as any representation or warranty that the insurance coverage and limits necessarily will be adequate to protect Contractor.

5. These and all other insurance requirements under the Contract apply to both Contractor and its Subcontractors, if any. Contractor is responsible for ensuring its Subcontractors' compliance with all requirements.

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE FOR HHSC STATEMENT OF WORK CONTRACT NO. HHS[xxxxxxxxx] under DIR DBITS Contract No. DIR-TSO-[xxxx]

Health and Human Services Commission	**CONTRACTOR*** **
SIGNATURE	SIGNATURE
PRINTED NAME	PRINTED NAME
TITLE	TITLE
DATE OF EXECUTION	DATE OF EXECUTION

NOTE: EXHIBITS AND ATTACHMENTS WILL BE ADDED DURING CONTRACT DEVELOPMENT. THE FOLLOWING LIST IS JUST AN EXAMPLE
EXHIBIT A – FINAL STATEMENT OF WORK. INCLUDING THE FOLLOWING:

1) **HHSC GENERAL AFFIRMATIONS**
2) **MODIFIED VENDOR INSURANCE COVERAGE**
3) **HHSC UNIFORM TERMS AND CONDITIONS**
4) **HHSC SPECIAL CONDITIONS**
5) **HHSC DATA USE AGREEMENT (DUA) AND SECURITY AND PRIVACY INITIAL INQUIRY (SPI)**
6) **LOBBYING CERTIFICATION**
7) **FEDERAL ASSURANCES - NON-CONSTRUCTION**
8) **FFATA CERTIFICATION**

EXHIBIT B - SERVICES RATE SCHEDULE
EXHIBIT C– DELIVERABLE COST SCHEDULE

Exhibit C1: Uniform Terms and Conditions

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Health and Human Services Commission

HHSC Uniform Terms and Conditions - Vendor

Version 2.15

Published and Effective September 1, 2017

Responsible Office: Chief Counsel

TABLE OF CONTENTS

Article I. Definitions and Interpretations 4
1.1 Definitions 4
1.2 Interpretive Provisions 5
Article II. Consideration 6
2.1 Prompt Payment 6
2.2 Expenses 6
2.3 Work Orders 6
Article III. State and Federal Funding 7
3.1 Funding 7
3.2 No debt Against the State 7
3.3 Debt to State 7
3.4 Recapture of Funds 7
Article IV. Warranty, Affirmations, Assurances and Certifications 8
4.1 Warranty 8
4.2 General Affirmations 8
4.3 Federal Assurances 8
4.4 Federal Certifications 8
Article V. Ownership and Intellectual Property 9
5.1 Ownership 9
5.2 Intellectual Property 9
Article VI. Records, Audit, and Disclosure 9
6.1 Books and Records 9
6.2 Access to records, books, and documents 9
6.3 Response/compliance with audit or inspection findings 10
6.4 SAO Audit 10
6.5 Confidentiality 10
6.6 Public Information Act 11
Article VII. Contract Management and Early Termination 11
7.1 Contract Management 11

7.2 Termination for Convenience 11
7.3 Termination for Cause 11
7.4 Contractor responsibility for associated costs. 12
7.5 Equitable Settlement 12
Article VIII. Miscellaneous Provisions 12
8.1 Amendment 12
8.2 Insurance 12
8.3 Delegation of Authority 12
8.4 Legal Obligations 13
8.5 E-Verify 13
8.6 Permitting and Licensure 13
8.7 Indemnity 13
8.8 Assignments 14
8.9 Subcontracts 14
8.10 HUB/Mentor Protégé 15
8.11 Relationship of the Parties 15
8.12 Technical Guidance Letters 16
8.13 Governing Law and Venue 16
8.14 Severability 16
8.15 Survivability 16
8.16 Force Majeure 16
8.17 Dispute Resolution 17
8.18.2017No Waiver of Provisions 17
8.19 Publicity 17
8.20 Prohibition on Non-compete Restrictions 17
8.21 No Waiver of Sovereign Immunity 17
8.22 Entire Contract and Modification 17
8.23 Counterparts 18
8.24 Proper Authority 18
8.25 Civil Rights 18

8.26 Enterprise Information Management Standards 19
8.27 Notice of Legal Matter or Litigation 19

ARTICLE I. DEFINITIONS AND INTERPRETATIONS

1.1 DEFINITIONS

As used in this Contract, unless the context clearly indicates otherwise, the following terms and conditions have the meanings assigned below:

"Amendment" means a written agreement, signed by the parties hereto, which documents changes to the Contract other than those permitted by Work Orders or Technical Guidance Letters, as herein defined.

"Attachment" means documents, terms, conditions, or additional information physically added to this Contract following the Signature Document or included by reference, as if physically, within the body of this Contract.

"Contract" means the Signature Document, these Uniform Terms and Conditions, along with any Attachments, and any Amendments, purchase orders, Work Orders, or Technical Guidance Letters that may be issued by the System Agency, to be incorporated by reference herein for all purposes if issued.

"Contractor" means the Party selected to provide the goods or services under this Contract, if any.

"Deliverable" means a work product prepared, developed, or procured by Contractor as part of the Services under the Contract for the use or benefit of the System Agency or the State of Texas.

"Effective Date" means the date agreed to by the Parties as the date on which the Contract takes effect.

"Federal Fiscal Year" means the period beginning October 1 and ending September 30 each year, which is the annual accounting period for the United States government.

"GAAP" means Generally Accepted Accounting Principles.

"GASB" means the Governmental Accounting Standards Board.

"Health and Human Services Commission" or "HHSC" means the administrative agency established under Chapter 531, Texas Government Code or its designee.

"HUB" means Historically Underutilized Business, as defined by Chapter 2161 of the Texas Government Code.

"Intellectual Property" means patents, rights to apply for patents, trademarks, trade names, service marks, domain names, copyrights and all applications and worldwide registration of such, schematics, industrial models, inventions, know-how, trade secrets, computer software

programs, and other intangible proprietary information. "Mentor Protégé" means the Comptroller of Public Accounts' leadership program found at:
http://www.window.state.tx.us/procurement/prog/hub/mentorprotege/.

"Parties" means the System Agency and Contractor, collectively.

"Party" means either the System Agency or Contractor, individually.

"Project" means the goods or Services described in the Signature Document or a Work Order of this Contract.

"Public Information Act" or "PIA" means Chapter 552 of the Texas Government Code.

"Scope of Work" means the description of Services and Deliverables specified in the Contract as may be amended.

"Services" means the tasks, functions, and responsibilities assigned and delegated to Contractor under the Contract.

"Signature Document" means the document executed by both Parties that specifically sets forth all of the documents that constitute the Contract.

"Solicitation" means the document issued by the System Agency under which the goods or services provided under the Contract were initially requested, which is incorporated herein by reference for all purposes in its entirety, including all Amendments and Attachments. "Solicitation Response" means Contractor's full and complete response to the Solicitation, which is incorporated herein by reference for all purposes in its entirety, including any Attachments and addenda.

"State Fiscal Year" means the period beginning September 1 and ending August 31 each year, which is the annual accounting period for the State of Texas.

"State of Texas *Textravel*" means Texas Administrative Code, Title 34, Part 1, Chapter 5, Subchapter C, Section 5.22, relative to travel reimbursements under this Contract, if any.

"Subcontract" means any written agreement between Contractor and a third party to fulfill the requirements of the Contract. All Subcontracts are required to be in writing.

"Subcontractor" means any individual or entity that enters a contract with the Contractor to perform part or all of the obligations of Contractor under this Contract.

"System Agency" means HHSC or any of the agencies of the State of Texas that are overseen by HHSC under authority granted under State law and the officers, employees, and designees of those agencies. These agencies include: HHSC and the Department of State Health Services.

"Technical Guidance Letter" or "TGL" means an instruction, clarification, or interpretation of the requirements of the Contract, issued by the System Agency to the Contractor.

"Work" means all Services to be performed, goods to be delivered, and any appurtenant actions performed and items produced, conceived, or developed, including Deliverables.

"Work Order" means an individually negotiated document that is executed by both Parties and which authorizes a Project, if any, in an indefinite quantity Contract.

1.2 INTERPRETIVE PROVISIONS

a. The meanings of defined terms are equally applicable to the singular and plural forms of the defined terms.

b. The words "hereof," "herein," "hereunder," and similar words refer to this Contract as a whole and not to any particular provision, section, Attachment, or schedule of this Contract unless otherwise specified.

c. The term "including" is not limiting and means "including without limitation" and, unless otherwise expressly provided in this Contract, (i) references to contracts (including this Contract) and other contractual instruments shall be deemed to include all subsequent Amendments and other modifications thereto, but only to the extent that such Amendments and other modifications are not prohibited by the terms of this Contract, and (ii) references to any statute or regulation are to be construed as including all statutory and regulatory provisions consolidating, amending, replacing, supplementing, or interpreting the statute or regulation.

d. Any references to "sections," "appendices," or "attachments" are references to sections, appendices, or attachments of the Contract.

e. Any references to agreements, contracts, statutes, or administrative rules or regulations in the Contract are references to these documents as amended, modified, or supplemented from time to time during the term of the Contract.

f. The captions and headings of this Contract are for convenience of reference only and do not affect the interpretation of this Contract.

g. All Attachments within this Contract, including those incorporated by reference, and any Amendments are considered part of the terms of this Contract.

h. This Contract may use several different limitations, regulations, or policies to regulate the same or similar matters. All such limitations, regulations, and policies are cumulative and each will be performed in accordance with its terms.

i. Unless otherwise expressly provided, reference to any action of the System Agency or by the System Agency by way of consent, approval, or waiver will be deemed modified by the phrase "in its sole discretion."

j. Time is of the essence in this Contract.

ARTICLE II. CONSIDERATION

2.1 PROMPT PAYMENT

The System Agency will pay Contractor in accordance with the Prompt Payment Act, Texas Government Code, Chapter 2251.

2.2 EXPENSES

Except as otherwise provided in the Contract, no ancillary expenses incurred by the Contractor in connection with its provision of the Services or Deliverables will be

reimbursed by the System Agency. Ancillary expenses include, but are not limited to costs associated with transportation, delivery, and insurance for each Deliverable.

When the reimbursement of travel expenses is authorized by the Contract, all such expenses will be reimbursed in accordance with the rates set by the State of Texas Textravel.

2.3 WORK ORDERS

To the extent the Contract is for indefinite quantities of services, as specified in the Signature Document, all Work will be performed in accordance with Work Orders.

a. Upon identification of a Project, the System Agency will request that Contractor submit a proposal, including pricing and a project plan, to System Agency.

b. If Contractor is selected to carry out an individual Project, a Work Order will be issued. Multiple Work Orders may be issued during the term of this Contract, all of which will be in writing and signed by the Parties. Each Work Order will include a scope of services; a list of tasks required; a time schedule; a list of Deliverables, if any; a detailed Project budget; and such other information or special conditions as may be necessary for the work assigned.

c. Nothing in this Contract expresses or guarantees that the System Agency will issue Work Orders to Contractor for any of the tasks set forth in the Signature Document. All work requested under this Contract will be required on an irregular and as needed basis throughout the Contract term, and the System Agency makes no guarantee of volume or usage under this Contract.

ARTICLE III. STATE AND FEDERAL FUNDING

3.1 FUNDING

This Contract is contingent upon the availability of sufficient and adequate funds. If funds become unavailable through lack of appropriations, budget cuts, transfer of funds between programs or agencies, amendment of the Texas General Appropriations Act, agency consolidation, or any other disruptions of current funding for this Contract, the System Agency may restrict, reduce, or terminate funding under this Contract. This Contract is also subject to immediate cancellation or termination, without penalty to the System Agency, if sufficient and adequate funds are not available. Contractor will have no right of action against the System Agency if the System Agency cannot perform its obligations under this Contract as a result of lack of funding for any activities or functions contained within the scope of this Contract. In the event of cancellation or termination under this Section, the System Agency will not be required to give notice and will not be liable for any damages or losses caused or associated with such termination or cancellation.

3.2 NO DEBT AGAINST THE STATE

The Contract will not be construed as creating any debt by or on behalf of the State of Texas.

3.3 DEBT TO STATE

If a payment law prohibits the Texas Comptroller of Public Accounts from making a payment, the Contractor acknowledges the System Agency's payments under the Contract will be applied toward eliminating the debt or delinquency. This requirement specifically applies to any debt or delinquency, regardless of when it arises.

3.4 RECAPTURE OF FUNDS

The System Agency may withhold all or part of any payments to Contractor to offset overpayments made to the Contractor. Overpayments as used in this Section include payments (i) made by the System Agency that exceed the maximum allowable rates; (ii) that are not allowed under applicable laws, rules, or regulations; or (iii) that are otherwise inconsistent with this Contract, including any unapproved expenditures. Contractor understands and agrees that it will be liable to the System Agency for any costs disallowed pursuant to financial and compliance audit(s) of funds received under this Contract. Contractor further understands and agrees that reimbursement of such disallowed costs will be paid by Contractor from funds which were not provided or otherwise made available to Contractor under this Contract.

ARTICLE IV. WARRANTY, AFFIRMATIONS, ASSURANCES AND CERTIFICATIONS

4.1 WARRANTY

Contractor warrants that all Work under this Contract will be completed in a manner consistent with standards under the terms of this Contract, in the applicable trade, profession, or industry; will conform to or exceed the specifications set forth in the Contract; and will be fit for ordinary use, of good quality, and with no material defects. If Contractor fails to complete Work timely or to perform satisfactorily under conditions required by this Contract, the System Agency may require Contractor, at its sole expense, to:

a. Repair or replace all defective or damaged Work;
b. Refund any payment received for all defective or damaged Work and, in conjunction therewith, require Contractor to accept the return of such Work; and
c. Take necessary action to ensure that future performance and Work conform to the Contract requirements.

4.2 GENERAL AFFIRMATIONS

Contractor further certifies that, to the extent General Affirmations are incorporated into the Contract under the Signature Document, the General Affirmations have been reviewed and that Contractor is in compliance with each of the requirements reflected therein.

4.3 FEDERAL ASSURANCES

Contractor further certifies that, to the extent Federal Assurances are incorporated into the Contract under the Signature Document, the Federal Assurances have been reviewed and that Contractor is in compliance with each of the requirements reflected therein.

4.4 FEDERAL CERTIFICATIONS

Contractor further certifies, to the extent Federal Certifications are incorporated into the Contract under the Signature Document, that the Federal Certifications have been reviewed, and that Contractor is in compliance with each of the requirements reflected therein. **In addition, Contractor certifies that it is in compliance with all applicable federal laws, rules, or regulations, as they may pertain to this Contract.**

ARTICLE V. OWNERSHIP AND INTELLECTUAL PROPERTY

5.1 OWNERSHIP

The System Agency will own, and Contractor hereby assigns to the System Agency, all right, title, and interest in all Work.

5.2 INTELLECTUAL PROPERTY

a. To the extent any Work results in the creation of Intellectual Property, all right, title, and interest in and to such Intellectual Property will vest in the System Agency upon creation and will be deemed to be a "work made for hire" and made in the course of the services rendered pursuant to this Contract.
b. To the extent that title to any such Intellectual Property may not by law vest in the System Agency, or such Intellectual Property may not be considered a "work made for hire," all rights, title, and interest therein are hereby irrevocably assigned to the System Agency. The System Agency will have the right to obtain and to hold in its name any and all patents, copyrights, trademarks, service marks, registrations, or such other protection as may be appropriate to the subject matter, including extensions and renewals thereof.
c. Contractor must give the System Agency and the State of Texas, as well as any person designated by the System Agency or the State of Texas, all assistance required to perfect the rights defined herein without any charge or expense beyond the stated amount payable to Contractor for the services authorized under this Contract.

ARTICLE VI. RECORDS, AUDIT, AND DISCLOSURE

6.1 BOOKS AND RECORDS

Contractor will keep and maintain under GAAP or GASB, as applicable, full, true, and complete records necessary to fully disclose to the System Agency, the Texas State Auditor's Office, the United States Government, and their authorized representatives sufficient information to determine compliance with the terms and conditions of this Contract and all state and federal rules, regulations, and statutes. Unless otherwise specified in this Contract, Contractor will maintain legible copies of this Contract and

all related documents for a minimum of seven (7) years after the termination of the contract period or seven (7) years after the completion of any litigation or dispute involving the Contract, whichever is later.

6.2 ACCESS TO RECORDS, BOOKS, AND DOCUMENTS

In addition to any right of access arising by operation of law, Contractor and any of Contractor's affiliate or subsidiary organizations, or Subcontractors will permit the System Agency or any of its duly authorized representatives, as well as duly authorized federal, state or local authorities, unrestricted access to and the right to examine any site where business is conducted or Services are performed, and all records, which includes but is not limited to financial, client and patient records, books, papers or documents related to this Contract. If the Contract includes federal funds, federal agencies that will have a right of access to records as described in this section include: the federal agency providing the funds, the Comptroller General of the United States, the General Accounting Office, the Office of the Inspector General, and any of their authorized representatives. In addition, agencies of the State of Texas that will have a right of access to records as described in this section include: the System Agency,
HHSC, HHSC's contracted examiners, the State Auditor's Office, the Texas Attorney General's Office, and any successor agencies. Each of these entities may be a duly authorized authority. If deemed necessary by the System Agency or any duly authorized authority, for the purpose of investigation or hearing, Contractor will produce original documents related to this Contract. The System Agency and any duly authorized authority will have the right to audit billings both before and after payment, and all documentation that substantiates the billings. Contractor will include this provision concerning the right of access to, and examination of, sites and information related to this Contract in any Subcontract it awards.

6.3 RESPONSE/COMPLIANCE WITH AUDIT OR INSPECTION FINDINGS

a. Contractor must act to ensure its and its Subcontractor's compliance with all corrections necessary to address any finding of noncompliance with any law, regulation, audit requirement, or generally accepted accounting principle, or any other deficiency identified in any audit, review, or inspection of the Contract and the goods or services provided hereunder. Any such correction will be at Contractor or its Subcontractor's sole expense. Whether Contractor's action corrects the noncompliance will be solely the decision of the System Agency.

b. As part of the Services, Contractor must provide to HHSC upon request a copy of those portions of Contractor's and its Subcontractors' internal audit reports relating to the Services and Deliverables provided to the State under the Contract.

6.4 SAO AUDIT

Contractor understands that acceptance of funds directly under the Contract or indirectly through a Subcontract under the Contract acts as acceptance of the authority of the State Auditor's Office (SAO), or any successor agency, to conduct an audit or investigation

in connection with those funds. Under the direction of the legislative audit committee, an entity that is the subject of an audit or investigation by the SAO must provide the SAO with access to any information the SAO considers relevant to the investigation or audit. Contractor agrees to cooperate fully with the SAO or its successor in the conduct of the audit or investigation, including providing all records requested. Contractor will ensure that this clause concerning the authority to audit funds received indirectly by Subcontractors through Contractor and the requirement to cooperate is included in any Subcontract it awards.

6.5 CONFIDENTIALITY

Any specific confidentiality agreement between the Parties takes precedent over the terms of this section. To the extent permitted by law, Contractor agrees to keep all information confidential, in whatever form produced, prepared, observed, or received by Contractor. The provisions of this section remain in full force and effect following termination or cessation of the services performed under this Contract.

6.6 PUBLIC INFORMATION ACT

Information related to the performance of this Contract may be subject to the PIA and will be withheld from public disclosure or released only in accordance therewith. Contractor must make all information not otherwise excepted from disclosure under the PIA available in portable document file (".pdf") format or any other format agreed between the Parties.

ARTICLE VII. CONTRACT MANAGEMENT AND EARLY TERMINATION

7.1 CONTRACT MANAGEMENT

To ensure full performance of the Contract and compliance with applicable law, the System Agency may take actions including:

a. Suspending all or part of the Contract;
b. Requiring the Contractor to take specific corrective actions in order to remain in compliance with term of the Contract;
c. Recouping payments made to the Contractor found to be in error;
d. Suspending, limiting, or placing conditions on the continued performance of Work;
e. Imposing any other remedies authorized under this Contract; and
f. Imposing any other remedies, sanctions or penalties permitted by federal or state statute, law, regulation, or rule.

7.2 TERMINATION FOR CONVENIENCE

The System Agency may terminate the Contract, in whole or in part, at any time when, in its sole discretion, the System Agency determines that termination is in the best interests of the State of Texas. The termination will be effective on the date specified in HHSC's notice of termination.

7.3 TERMINATION FOR CAUSE

Except as otherwise provided by the U.S. Bankruptcy Code, or any successor law, the System Agency may terminate the Contract, in whole or in part, upon either of the following conditions:

a. **Material Breach**

The System Agency will have the right to terminate the Contract in whole or in part if the System Agency determines, at its sole discretion, that Contractor has materially breached the Contract or has failed to adhere to any laws, ordinances, rules, regulations or orders of any public authority having jurisdiction and such violation prevents or substantially impairs performance of Contractor's duties under the Contract. Contractor's misrepresentation in any aspect of Contractor's Solicitation Response, if any, or Contractor's addition to the Excluded Parties List System (EPLS) will also constitute a material breach of the Contract.

b. **Failure to Maintain Financial Viability**

The System Agency may terminate the Contract if, in its sole discretion, the System Agency has a good faith belief that Contractor no longer maintains the financial viability required to complete the Services and Deliverables, or otherwise fully perform its responsibilities under the Contract.

7.4 CONTRACTOR RESPONSIBILITY FOR ASSOCIATED COSTS.

If the System Agency terminates the Contract for Cause, the Contractor will be responsible to the System Agency for all costs incurred by the System Agency and the State of Texas to replace the Contractor. These costs include, but are not limited to, the costs of procuring a substitute vendor and the cost of any claim or litigation that is reasonably attributable to Contractor's failure to perform any Work in accordance with the terms of the Contract.

7.5 EQUITABLE SETTLEMENT

Any early termination under this Article will be subject to the equitable settlement of the respective interests of the Parties up to the date of termination.

ARTICLE VIII. MISCELLANEOUS PROVISIONS

8.1 AMENDMENT

The Contract may only be amended by an Amendment executed by both Parties.

8.2 INSURANCE

Unless otherwise specified in this Contract, Contractor will acquire and maintain, for the duration of this Contract, insurance coverage necessary to ensure proper fulfillment of this Contract and potential liabilities thereunder with financially sound and reputable insurers licensed by the Texas Department of Insurance, in the type and amount customarily carried within the industry as determined by the System Agency. Contractor will provide evidence of insurance as required under this Contract, including a schedule

of coverage or underwriter's schedules establishing to the satisfaction of the System Agency the nature and extent of coverage granted by each such policy, upon request by the System Agency. In the event that any policy is determined by the System Agency to be deficient to comply with the terms of this Contract, Contractor will secure such additional policies or coverage as the System Agency may reasonably request or that are required by law or regulation. If coverage expires during the term of this Contract, Contractor must produce renewal certificates for each type of coverage.

These and all other insurance requirements under the Contract apply to both Contractor and its Subcontractors, if any. Contractor is responsible for ensuring its Subcontractors' compliance with all requirements.

8.3 Delegation of Authority

Whenever, by any provision of the Contract, any right, power or duty is imposed or conferred on HHSC, the right power or duty so imposed or conferred is possessed and exercised by the System Agencies Executive Commissioner unless such is delegated to duly appointed agents or employees. The Executive Commissioner of the System Agency will reduce any delegation of authority to writing and provide a copy to Contractor on request. The authority delegated to Contractor by the System Agency is limited to the terms of the Contract. Contractor may not reply upon implied authority and is not delegated authority under the Contract to:

a. Make public policy;
b. Promulgate, amend, or disregard administrative regulations or program policy decisions made by State and federal agencies responsible for administration of System Agency program; or
c. Unilaterally communicate or negotiate with any federal or state agency or the Texas Legislature on behalf of the System Agency regarding the System Agency programs or the Contract. However, upon request and reasonable notice to the Contractor, Contract will assist the System Agency in communications and negotiations regarding the Work under the Contract with state and federal governments.

8.4 Legal Obligations

Contractor will comply with all applicable federal, state, and local laws, ordinances, and regulations, including all federal and state accessibility laws relating to direct and indirect use of information and communication technology. Contractor will be deemed to have knowledge of all applicable laws and regulations and be deemed to understand them. In addition to any other act or omission that may constitute a material breach of the Contract, failure to comply with this Section may also be a material breach of the Contract.

8.5 E-Verify

By entering into this Contract, Contractor certifies and ensures that it utilizes and will continue to utilize, for the term of this Contract, the U.S. Department of Homeland Security's e-Verify system to determine the eligibility of:

a. All persons employed during the contract term to perform duties within Texas; and
b. All persons (including subcontractors) assigned by the contractor to perform Work pursuant to the Contract.

8.6 PERMITTING AND LICENSURE

At Contractor's sole expense, Contractor will procure and maintain for the duration of this Contract any state, county, city, or federal license, authorization, insurance, waiver, permit, qualification or certification required by statute, ordinance, law, or regulation to be held by Contractor to provide the goods or Services required by this Contract. Contractor will be responsible for payment of all taxes, assessments, fees, premiums, permits, and licenses required by law. Contractor agrees to be responsible for payment of any such government obligations not paid by its Subcontractors during performance of this Contract.

8.7 INDEMNITY

TO THE EXTENT ALLOWED BY LAW, CONTRACTOR WILL DEFEND, INDEMNIFY, AND HOLD HARMLESS THE STATE OF TEXAS AND ITS OFFICERS AND EMPLOYEES, AND THE SYSTEM AGENCY AND ITS OFFICERS AND EMPLOYEES, FROM AND AGAINST ALL CLAIMS, ACTIONS, SUITS, DEMANDS, PROCEEDINGS, COSTS, DAMAGES, AND LIABILITIES, INCLUDING ATTORNEYS' FEES AND COURT COSTS ARISING OUT OF, OR CONNECTED WITH, OR RESULTING FROM:

- **CONTRACTOR'S PERFORMANCE OF THE CONTRACT, INCLUDING ANY NEGLIGENT ACTS OR OMISSIONS OF CONTRACTOR, OR ANY AGENT, EMPLOYEE, SUBCONTRACTOR, OR SUPPLIER OF CONTRACTOR, OR ANY THIRD PARTY UNDER THE CONTROL OR SUPERVISION OF CONTRACTOR, IN THE EXECUTION OR PERFORMANCE OF THIS CONTRACT; OR**
- **ANY BREACH OR VIOLATION OF A STATUTE, ORDINANCE, GOVERNMENTAL REGULATION, STANDARD, RULE, OR BREACH OF CONTRACT BY CONTRACTOR, ANY AGENT, EMPLOYEE, SUBCONTRACTOR, OR SUPPLIER OF CONTRACTOR, OR ANY THIRD PARTY UNDER THE CONTROL OR SUPERVISION OF CONTRACTOR, IN THE EXECUTION OR PERFORMANCE OF THIS CONTRACT; OR**
- **EMPLOYMENT OR ALLEGED EMPLOYMENT, INCLUDING CLAIMS OF DISCRIMINATION AGAINST CONTRACTOR, ITS OFFICERS, OR ITS AGENTS; OR**
- **WORK UNDER THIS CONTRACT THAT INFRINGES OR MISAPPROPRIATES ANY RIGHT OF ANY THIRD PERSON OR ENTITY BASED ON COPYRIGHT, PATENT, TRADE SECRET, OR OTHER INTELLECTUAL PROPERTY RIGHTS.**

CONTRACTOR WILL COORDINATE ITS DEFENSE WITH THE SYSTEM AGENCY AND ITS COUNSEL. THIS PARAGRAPH IS NOT INTENDED TO AND WILL NOT BE CONSTRUED TO REQUIRE CONTRACTOR TO INDEMNIFY OR HOLD HARMLESS THE STATE OR THE SYSTEM AGENCY FOR ANY CLAIMS OR LIABILITIES RESULTING SOLELY FROM THE

GROSS NEGLIGENCE OF THE SYSTEM AGENCY OR ITS EMPLOYEES. THE PROVISIONS OF THIS SECTION WILL SURVIVE TERMINATION OF THIS CONTRACT.

8.8 ASSIGNMENTS

Contractor may not assign all or any portion of its rights under, interests in, or duties required under this Contract without prior written consent of the System Agency, which may be withheld or granted at the sole discretion of the System Agency. Except where otherwise agreed in writing by the System Agency, assignment will not release Contractor from its obligations under the Contract.

Contractor understands and agrees the System Agency may in one or more transactions assign, pledge, or transfer the Contract. This assignment will only be made to another State agency or a non-state agency that is contracted to perform agency support.

8.9 SUBCONTRACTS

Contractor will be responsible to the System Agency for any Subcontractor's performance under this Contract. Nothing in this Contract will be construed to relieve Contractor of the responsibility for ensuring that the goods delivered or services rendered by Contractor or any of its Subcontractors comply with all the terms and provisions of this Contract. Contractor will provide written notification to the System Agency of any Subcontractor receiving compensation of One hundred thousand dollars ($100,000.00) or more of the Work under this Contract, including the name and taxpayer identification number of Subcontractor, the task(s) being performed, and the number of Subcontractor employees expected to perform Services. The System Agency reserves the right to:

a. Reject the Subcontract or require changes to any provisions that do not comply with the requirements, duties, or responsibilities of the Contract or that create significant barriers for the System Agency to monitor compliance with the Contract;
b. Object to the selection of the Subcontractor; or
c. Object to the subcontracting of the Work proposed to be Subcontracted.

8.10 HUB/MENTOR PROTÉGÉ

In accordance with State law, it is the System Agency's policy to assist HUBs whenever possible in providing goods and services to the System Agency. The System Agency encourages those parties with whom it contracts for the provision of goods and services to adhere to this same philosophy in selecting Subcontractors to assist in fulfilling their obligations with the System Agency. In addition to information required by this Contract, the contracting Party will provide the procurement department of the System Agency with pertinent details of any participation by a HUB in fulfilling the duties and obligations arising hereunder.

The System Agency encourages the Parties it contracts with to partner with certified HUBs that participate in the Texas Comptroller of Public Accounts' Mentor Protégé Program.

8.11 RELATIONSHIP OF THE PARTIES

Contractor is, and will be, an independent contractor and, subject only to the terms of this Contract, will have the sole right to supervise, manage, operate, control, and direct performance of the details incident to its duties under this Contract. Nothing contained in this Contract will be deemed or construed to create a partnership or joint venture, to create relationships of an employer-employee or principal-agent, or to otherwise create for the System Agency any liability whatsoever with respect to the indebtedness, liabilities, and obligations of Contractor or any other Party.

Contractor will be solely responsible for, and the System Agency will have no obligation with respect to:

a. Payment of Contractor's employees for all Services performed;
b. Ensuring each of its employees, agents, or Subcontractors who provide Services or Deliverables under the Contract are properly licensed, certified, or have proper permits to perform any activity related to the Work;
c. Withholding of income taxes, FICA, or any other taxes or fees;
d. Industrial or workers' compensation insurance coverage;
e. Participation in any group insurance plans available to employees of the State of Texas;
f. Participation or contributions by the State to the State Employees Retirement System;
g. Accumulation of vacation leave or sick leave; or
h. Unemployment compensation coverage provided by the State.

8.12 TECHNICAL GUIDANCE LETTERS

In the sole discretion of the System Agency, and in conformance with federal and state law, the System Agency may issue instructions, clarifications, or interpretations as may be required during Work performance in the form of a Technical Guidance Letter. A TGL must be in writing, and may be delivered by regular mail, electronic mail, or facsimile transmission. Any TGL issued by the System Agency will be incorporated into the Contract by reference herein for all purposes when it is issued.

8.13 GOVERNING LAW AND VENUE

This Contract and the rights and obligations of the Parties hereto will be governed by, and construed according to, the laws of the State of Texas, exclusive of conflicts of law provisions. Venue of any suit brought under this Contract will be in a court of competent jurisdiction in Travis County, Texas unless otherwise elected by the System Agency. Contractor irrevocably waives any objection, including any objection to personal jurisdiction or the laying of venue or based on the grounds of forum non conveniens, which it may now or hereafter have to the bringing of any action or proceeding in such jurisdiction in respect of this Contract or any document related hereto.

8.14 SEVERABILITY

If any provision contained in this Contract is held to be unenforceable by a court of law or equity, this Contract will be construed as if such provision did not exist and the nonenforceability of such provision will not be held to render any other provision or provisions of this Contract unenforceable.

8.15 SURVIVABILITY

Termination or expiration of this Contract or a Contract for any reason will not release either party from any liabilities or obligations in this Contract that the parties have expressly agreed will survive any such termination or expiration, remain to be performed, or by their nature would be intended to be applicable following any such termination or expiration, including maintaining confidentiality of information and records retention.

8.16 FORCE MAJEURE

Except with respect to the obligation of payments under this Contract, if either of the Parties, after a good faith effort, is prevented from complying with any express or implied covenant of this Contract by reason of war; terrorism; rebellion; riots; strikes; acts of God; any valid order, rule, or regulation of governmental authority; or similar events that are beyond the control of the affected Party (collectively referred to as a "Force Majeure"), then, while so prevented, the affected Party's obligation to comply with such covenant will be suspended, and the affected Party will not be liable for damages for failure to comply with such covenant. In any such event, the Party claiming Force Majeure will promptly notify the other Party of the Force Majeure event in writing and, if possible, such notice will set forth the extent and duration thereof.

8.17DISPUTE RESOLUTION

If a contract dispute arises that cannot be resolved to the satisfaction of the Parties, either Party may notify the other Party in writing of the dispute. If the Parties are unable to satisfactorily resolve the dispute within fourteen (14) days of the written notification, the Parties must use the dispute resolution process provided for in Chapter 2260 of the Texas Government Code to attempt to resolve the dispute. This provision will not apply to any matter with respect to which either Party may make a decision within its respective sole discretion.

8.18.2017NO WAIVER OF PROVISIONS

Neither failure to enforce any provision of this Contract nor payment for services provided under it constitute waiver of any provision of the Contract.

8.19 PUBLICITY

Except as provided in the paragraph below, Contractor must not use the name of, or directly or indirectly refer to, the System Agency, the State of Texas, or any other State agency in any media release, public announcement, or public disclosure relating to the Contract or its subject matter, including in any promotional or marketing materials, customer lists, or business presentations.

Contractor may publish, at its sole expense, results of Contractor performance under the Contract with the System Agency's prior review and approval, which the System Agency may exercise at its sole discretion. Any publication (written, visual, or sound) will acknowledge the support received from the System Agency and any Federal agency, as appropriate.

8.20 Prohibition on Non-compete Restrictions

Contractor will not require any employees or Subcontractors to agree to any conditions, such as non-compete clauses or other contractual arrangements that would limit or restrict such persons or entities from employment or contracting with the State of Texas.

8.21 No Waiver of Sovereign Immunity

Nothing in the Contract will be construed as a waiver of sovereign immunity by the System Agency.

8.22 Entire Contract and Modification

The Contract constitutes the entire agreement of the Parties and is intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Any additional or conflicting terms in any future document incorporated into the Contract will be harmonized with this Contract to the extent possible by the System Agency.

8.23Counterparts

This Contract may be executed in any number of counterparts, each of which will be an original, and all such counterparts will together constitute but one and the same Contract.

8.24 Proper Authority

Each Party hereto represents and warrants that the person executing this Contract on its behalf has full power and authority to enter into this Contract. Any Services or Work performed by Contractor before this Contract is effective or after it ceases to be effective are performed at the sole risk of Contractor with respect to compensation.

8.25 Civil Rights

a. Contractor agrees to comply with state and federal anti-discrimination laws, including:
   (1) Title VI of the Civil Rights Act of 1964 (42 U.S.C. §2000d *et seq.*);
   (2) Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. §794);
   (3) Americans with Disabilities Act of 1990 (42 U.S.C. §12101 *et seq.*);
   (4) Age Discrimination Act of 1975 (42 U.S.C. §§6101-6107);
   (5) Title IX of the Education Amendments of 1972 (20 U.S.C. §§1681-1688);
   (6) Food and Nutrition Act of 2008 (7 U.S.C. §2011 *et seq.*); and

(7) The System Agency's administrative rules, as set forth in the Texas Administrative Code, to the extent applicable to this Agreement.

Contractor agrees to comply with all amendments to these laws, and all requirements imposed by the regulations issued pursuant to these laws. These laws provide in part that no persons in the United States may, on the grounds of race, color, national origin, sex, age, disability, political beliefs, or religion, be excluded from participation in or denied any service or other benefit provided by Federal or State funding, or otherwise be subjected to discrimination.

b. Contractor agrees to comply with Title VI of the Civil Rights Act of 1964, and its implementing regulations at 45 C.F.R. Part 80 or 7 C.F.R. Part 15, prohibiting a contractor from adopting and implementing policies and procedures that exclude or have the effect of excluding or limiting the participation of clients in its programs, benefits, or activities on the basis of national origin. Civil rights laws require contractors to provide alternative methods for ensuring access to services for applicants and recipients who cannot express themselves fluently in English. Contractor agrees to take reasonable steps to provide services and information, both orally and in writing and electronically, in appropriate languages other than English, to ensure that persons with limited English proficiency are effectively informed and can have meaningful access to programs, benefits, and activities.

c. Contractor agrees to post applicable civil rights posters in areas open to the public informing clients of their civil rights and including contact information for

the HHS Civil Rights Office. The posters are available on the HHS website at: http://hhscx.hhsc.texas.gov/system-support-services/civil-rights/publications

d. Contractor agrees to comply with Executive Orders 13279 and 13559, and their implementing regulations at 45 C.F.R. Part 87 or 7 C.F.R. Part 16. These provide in part that any organization that participates in programs funded by direct financial assistance from the United States Department of Agriculture or the United States Department of Health and Human Services shall not discriminate against a program beneficiary or prospective program beneficiary on the basis of religion or religious belief. Contractor must provide written notice to beneficiaries of their rights.

e. Upon request, Contractor will provide HHSC Civil Rights Office with copies of the Contractor's civil rights policies and procedures.

f. Contractor must notify HHSC's Civil Rights Office of any civil rights complaints received relating to its performance under this Agreement. This notice must be delivered no more than ten (10) calendar days after receipt of a complaint. This notice must be directed to:

HHSC Civil Rights Office

701 W. 51st Street, Mail Code W206
Austin, Texas 78751
Phone Toll Free: (888) 388-6332
Phone: (512) 438-4313
TTY Toll Free: (877) 432-7232 Fax:
(512) 438-5885.

8.26 Enterprise Information Management Standards

Contractor agrees that it will conform to HHSC standards for data management as described by the policies of the HHSC Office of the Chief Data Officer (OCDO). These include, but are not limited to, standards for documentation and communication of data models, metadata, and other data definition methods that are required by the HHSC for ongoing data governance, strategic portfolio analysis, interoperability planning, and valuation of HHS System data assets.

8.27 Notice of Legal Matter or Litigation

Contractor shall notify the contract manager assigned to this Contract of any litigation or legal matter related to or affecting this Contract within seven calendar days of becoming aware of the litigation or legal matter.

Remainder of Page Intentionally Left Blank

Exhibit C2:
HHSC Special Conditions

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

Contents

Article I. Special Definitions 1

Article II. General Provisions 2

2.01 Other System Agencies Participation in the Contract 2
2.02 Most Favored Customer 2
2.03 Cooperation with HHSC Vendors 2
2.04 Renegotiation and Reprocurement Rights 2
2.05 Additional Provision regarding the Texas Public Information Act 3

Article III. Contractors Personnel and Subcontractors 3

3.01 Qualifications 3
3.02 Conduct and Removal 3

Article IV. Performance 3

4.01 Measurement 3

Article V. Amendments and Modifications 4

5.01 Formal Procedure 4
5.02 Minor Administrative Changes 4

Article VI. Payment 4

6.01 Enhanced Payment Procedures 4

Article VII. Confidentiality 5

7.01 Consultant Disclosure 5
7.02 Confidential System Information 5

Article VIII. Disputes and Remedies 5

8.01 Agreement of the Parties 5
8.02 Operational Remedies 6
8.03 Equitable Remedies 6
8.04 Continuing Duty to Perform 7

Article IX. Damages 7

9.01 Availability and Assessment 7
9.02 Specific Items of Liability 7

Article X. Additional License and Ownership Provisions 8

10.01 HHSC Additional Rights 8
10.02 Software and Ownership Rights 8

Article XI. Uniform ICT Accessibility Clause....8

11.01 Applicability.... 8
11.02 Definitions.... 8
11.03 Accessibility Requirements.... 9
11.04 Evaluation, Testing and Monitoring 9
11.05 Representations and Warranties.... 10
11.06 Remedies.... 10

Article XII. Miscellaneous Provisions 10

12.01 Conflicts of Interest.... 10
12.02 Flow Down Provisions.... 11
12.03 Manufacturer's Warranties.... 11

HHSC SPECIAL CONDITIONS

The terms and conditions of these Special Conditions are incorporated into and made a part of the Contract. Capitalized items used in these Special Conditions and not otherwise defined have the meanings assigned to them in HHSC Uniform Terms and Conditions –Vendor- Version 2.14

Article I. SPECIAL DEFINITIONS

"Conflict of Interest" means a set of facts or circumstances, a relationship, or other situation under which Contractor, a Subcontractor, or individual has past, present, or currently planned personal or financial activities or interests that either directly or indirectly: (1) impairs or diminishes the Contractor's, or Subcontractor's ability to render impartial or objective assistance or advice to the HHSC; or (2) provides the Contractor or Subcontractor an unfair competitive advantage in future HHSC procurements.

"Contractor Agents" means Contractor's representatives, employees, officers, Subcontractors, as well as their employees, contractors, officers, and agents.

"Custom Software" means Software developed as a Deliverable or in connection with the Agreement.

"Data Use Agreement" means the agreement incorporated into the Contract to facilitate creation, receipt, maintenance, use, disclosure or access to Confidential Information.

"Federal Financial Participation" is a program that allows states to receive partial reimbursement for activities that meet certain objectives of the federal government. It is also commonly referred to as the Federal Medical Assistance Percentage (FMAP).

"Item of Noncompliance" means Contractor's acts or omissions that: (1) violate a provision of the Contract; (2) fail to ensure adequate performance of the Work; (3) represent a failure of Contractor to be responsive to a request of HHSC relating to the Work under the Contract.

"Minor Administrative Change" refers to a change to the Contract that does not increase the fees or term and done in accordance with Section 6.02 of these Special Conditions.

"Confidential System Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to Contractor; or that Contractor may create, receive, maintain, use, disclose or have access to on behalf of HHSC or through performance of the Work, which is not designated as Confidential Information in a Data Use Agreement.

"State" means the State of Texas and, unless otherwise indicated or appropriate, will be interpreted to mean HHSC and other agencies of the State of Texas that may participate in the administration of HHSC Programs; provided, however, that no provision will be interpreted to include any entity other than HHSC as the contracting agency.

"Software" means all operating system and applications software used or created by Contractor to perform the Work under the Contract.

"Third Party Software" refers to software programs or plug-ins developed by companies or individuals other than Contractor which are used in performance of the Work. It does not include items which are ancillary to the performance of the Work, such as internal systems of Contractor which were deployed by Contractor prior to the Contract and not procured to perform the Work.

"UTC" means HHSC's Uniform Terms and Conditions- Vendor –Version 2.15

Article II. GENERAL PROVISIONS

2.01 Other System Agencies Participation in the Contract

In addition to providing the Work specified for HHSC, Contractor agrees to allow other System Agencies the option to participate in the Contract under the same terms and conditions. Each System Agency that elects to obtain Work under this section will issue a purchase or Work order to Contractor, referring to, and incorporating by reference, the terms and conditions specified in the Contract.

System Agencies have no authority to modify the terms of the Contract. However, additional System Agency terms and conditions that do not conflict with the Contract, and are acceptable to the Contractor, may be added in a purchase or Work order and given effect. No additional term or condition added in a purchase or Work order issued by a System Agency can conflict with or diminish a term or condition of the Contract. In the event of a conflict between a System Agency's purchase or Work order and the Contract, the Contract terms control.

2.02 Most Favored Customer

Contractor agrees that if during the term of the Contract, Contractor enters into any agreement with any other governmental customer, or any non-affiliated commercial customer by which it agrees to provide equivalent services at lower prices, or additional services at comparable prices, Contractor will notify HHSC within (10) business days from the date Contractor executes any such agreement. Contractor agrees, at HHSC's option, to amend the Contract to accord equivalent advantage to HHSC.

2.03 Cooperation with HHSC Vendors

At HHSC's request, Contractor will allow parties interested in responding to other HHSC solicitations to have reasonable access during normal business hours to the Work, software, systems documentation, and site visits to the Contractor's facilities. Contractor may elect to have such parties inspecting the Work, facilities, software or systems documentation to agree to use the information so obtained only in the State of Texas and only for the purpose of responding to the relevant HHSC solicitation.

2.04 Renegotiation and Reprocurement Rights

Notwithstanding anything in the Contract to the contrary, HHSC may at any time during the term of the Contract exercise the option to notify Contractor that HHSC has elected to renegotiate certain terms of the Contract. Upon Contractor's receipt of any notice under this section, Contractor and HHSC will undertake good faith negotiations of the subject terms of the Contract.

HHSC may at any time issue solicitation instruments to other potential contractors for performance of any portion of the Work covered by the Contract, including services similar or comparable to the Work, performed by Contractor under the Contract. If HHSC elects to procure the Work, or any portion thereof, from another vendor in accordance with this section, HHSC will have the termination rights set forth in the UTC.

2.05 Additional Provision regarding the Texas Public Information Act

The requirements of Subchapter J, Chapter 552, Government Code, may apply to this contract and the contractor or vendor agrees that the contract can be terminated if the contractor or vendor knowingly or intentionally fails to comply with a requirement of that subchapter.

Article III. CONTRACTORS PERSONNEL AND SUBCONTRACTORS

3.01 Qualifications

Contractor agrees to maintain the organizational and administrative capacity and capabilities proposed in its response to the Solicitation, as modified, to carry out all duties and responsibilities under the Contract. Contractor Agents assigned to perform the duties and responsibilities under the Contract must be and remain properly trained and qualified for the functions they are to perform. Notwithstanding the transfer or turnover of personnel, Contractor remains obligated to perform all duties and responsibilities under the Contract without degradation and in strict accordance with the terms of the Contract.

3.02 Conduct and Removal

While performing the Work under the Contract, Contractor Agents must comply with applicable Contract terms, State and federal rules, regulations, HHSC's policies, and HHSC's requests regarding personal and professional conduct; and otherwise conduct themselves in a businesslike and professional manner.

If HHSC determines in good faith that a particular Contractor Agent is not conducting himself or herself in accordance with the terms of the Contract, HHSC may provide Contractor with notice and documentation regarding its concerns. Upon receipt of such notice, Contractor must promptly investigate the matter and, at HHSC's election, take appropriate action that may include removing the Contractor Agent from performing any Work under the Contract and replacing the Contractor Agent with a similarly qualified individual acceptable to HHSC as soon as reasonably practicable or as otherwise agreed to by HHSC.

Article IV. PERFORMANCE

4.01 Measurement

Satisfactory performance of the Contract, unless otherwise specified in the Contract, will be measured by:

(a) Compliance with Contract requirements, including all representations and warranties;
(b) Compliance with the Work requested in the Solicitation and Work proposed by Contractor in its response to the Solicitation and approved by HHSC;

(c) Delivery of Work in accordance with the service levels proposed by Contractor in the Solicitation Response as accepted by HHSC;
(d) Results of audits, inspections, or quality checks performed by the HHSC or its designee;
(e) Timeliness, completeness, and accuracy of Work; and
(f) Achievement of specific performance measures and incentives as applicable.

Article V. AMENDMENTS AND MODIFICATIONS

5.01 Formal Procedure

No different or additional Work or contractual obligations will be authorized or performed unless contemplated within the Scope of Work and memorialized in an amendment or modification of the Contract that is executed in compliance with this Article. No waiver of any term, covenant, or condition of the Contract will be valid unless executed in compliance with this Article. Contractor will not be entitled to payment for Work that is not authorized by a properly executed Contract amendment or modification, or through the express written authorization of HHSC.

Any changes to the Contract that results in a change to either the term, fees, or significantly impacting the obligations of the parties to the Contract must be effectuated by a formal Amendment to the Contract. Such Amendment must be signed by the appropriate and duly authorized representative of each party in order to have any effect.

5.02 Minor Administrative Changes

HHSC's designee, referred to as the Contract Manager, Project Sponsor, or other equivalent, in the Contract, is authorized to provide written approval of mutually agreed upon Minor Administrative Changes to the Work or the Contract that do not increase the fees or term. Changes that increase the fees or term must be accomplished through the formal amendment procedure, as set forth in Section 6.01 of these Special Conditions. Upon approval of a Minor Administrative Change, HHSC and Contractor will maintain written notice that the change has been accepted in their Contract files.

Article VI. PAYMENT

6.01 Enhanced Payment Procedures

HHSC will be relieved of its obligation to make any payments to Contractor until such time as any and all set-off amounts have been credited to HHSC. If HHSC disputes payment of all or any portion of an invoice from Contractor, HHSC will notify the Contractor of the dispute and both Parties will attempt in good faith to resolve the dispute in accordance with these Special Conditions. HHSC will not be required to pay any disputed portion of a Contractor invoice unless, and until, the dispute is resolved. Notwithstanding any such dispute, Contractor will continue to perform the Work in compliance with the terms of the Contract pending resolution of such dispute so long as all undisputed amounts continue to be paid to Contractor.

Article VII. CONFIDENTIALITY

7.01 Consultant Disclosure

Contractor agrees that any consultant reports received by HHSC in connection with the Contract may be distributed by HHSC, in its discretion, to any other state agency and the Texas legislature. Any distribution may include posting on HHSC's website or the website of a standing committee of the Texas Legislature.

7.02 Confidential System Information

HHSC prohibits the unauthorized disclosure of Confidential System Information. Contractor and all Contractor Agents will not disclose or use any Confidential System Information in any manner except as is necessary for the Work or the proper discharge of obligations and securing of rights under the Contract. Contractor will have a system in effect to protect Confidential System Information. Any disclosure or transfer of Confidential System Information by Contractor, including information requested to do so by HHSC, will be in accordance with the Contract. If Contractor receives a request for Confidential System Information, Contractor will immediately notify HHSC of the request, and will make reasonable efforts to protect the Confidential System Information from disclosure until further instructed by the HHSC.

Contractor will notify HHSC promptly of any unauthorized possession, use, knowledge, or attempt thereof, of any Confidential System Information by any person or entity that may become known to Contractor. Contractor will furnish to HHSC all known details of the unauthorized possession, use, or knowledge, or attempt thereof, and use reasonable efforts to assist HHSC in investigating or preventing the reoccurrence of any unauthorized possession, use, or knowledge, or attempt thereof, of Confidential System Information.

HHSC will have the right to recover from Contractor all damages and liabilities caused by or arising from Contractor or Contractor Agents' failure to protect HHSC's Confidential Information as required by this section.

IN COORDINATION WITH THE INDEMNITY PROVISIONS CONTAINED IN THE UTC, Contractor WILL INDEMNIFY AND HOLD HARMLESS HHSC FROM ALL DAMAGES, COSTS, LIABILITIES, AND EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS' FEES AND COSTS) CAUSED BY OR ARISING FROM Contractor OR Contractor AGENTS FAILURE TO PROTECT CONFIDENTIAL SYSTEM INFORMATION. Contractor WILL FULFILL THIS PROVISION WITH COUNSEL APPROVED BY HHSC.

Article VIII. DISPUTES AND REMEDIES

8.01 Agreement of the Parties

The Parties agree that the interests of fairness, efficiency, and good business practices are best served when the Parties employ all reasonable and informal means to resolve any dispute under the Contract before resorting to formal dispute resolution processes otherwise provided in the Contract. The Parties will use all reasonable and informal means of resolving disputes prior to invoking a remedy provided elsewhere in the Contract, unless HHSC immediately terminates the Contract in accordance with the terms and conditions of the Contract.

Any dispute, that in the judgment of any Party to the Agreement, may materially affect the performance of any Party will be reduced to writing and delivered to the other Party within 10 business days after the dispute arises. The Parties must then negotiate in good faith and use every reasonable effort to resolve the dispute at the managerial or executive levels prior to initiating formal proceedings pursuant to the UTC and Texas Government Code §2260, unless a Party has reasonably determined that a negotiated resolution is not possible and has so notified the other Party. The resolution of any dispute disposed of by agreement between the Parties will be reduced to writing and delivered to all Parties within 10 business days of such resolution.

8.02 Operational Remedies

The remedies described in this section may be used or pursued by HHSC in the context of the routine operation of the Contract and are directed to Contractor's timely and responsive performance of the Work as well as the creation of a flexible and responsive relationship between the Parties. Contractor agrees that HHSC may pursue operational remedies for Items of Noncompliance with the Contract. At any time, and at its sole discretion, HHSC may impose or pursue one or more said remedies for each Item of Noncompliance. HHSC will determine operational remedies on a case-by-case basis which include, but are not, limited to:

(a) Requesting a detailed Corrective Action Plan, subject to HHSC approval, to correct and resolve a deficiency or breach of the Contract;
(b) Require additional or different corrective action(s) of HHSC's choice;
(c) Suspension of all or part of the Contract or Work;
(d) Prohibit Contractor from incurring additional obligations under the Contract;
(e) Issue Notice to stop Work Orders;
(f) Assessment of liquidated damages as provided in the Contract;
(g) Accelerated or additional monitoring;
(h) Withholding of payments; and
(i) Additional and more detailed programmatic and financial reporting.

HHSC's pursuit or non-pursuit of an operational remedy does not constitute a waiver of any other remedy that HHSC may have at law or equity; excuse Contractor's prior substandard performance, relieve Contractor of its duty to comply with performance standards, or prohibit HHSC from assessing additional operational remedies or pursuing other appropriate remedies for continued substandard performance.

HHSC will provide notice to Contractor of the imposition of an operational remedy in accordance with this section, with the exception of accelerated monitoring, which may be unannounced. HHSC may require Contractor to file a written response as part of the operational remedy approach.

8.03 Equitable Remedies

Contractor acknowledges that if, Contractor breaches, attempts, or threatens to breach, any obligation under the Contract, the State will be irreparably harmed. In such a circumstance, the State may proceed directly to court notwithstanding any other provision of the Contract. If a court of competent jurisdiction finds that Contractor breached, attempted, or threatened to breach any such obligations, Contractor will not oppose the entry of an order compelling performance by Contractor and restraining it from any further breaches, attempts, or threats of breach without a further finding of irreparable injury or other conditions to injunctive relief.

8.04 Continuing Duty to Perform

Neither the occurrence of an event constituting an alleged breach of contract, the pending status of any claim for breach of contract, nor the application of an operational remedy, is grounds for the suspension of performance, in whole or in part, by Contractor of the Work or any duty or obligation with respect to the Contract.

Article IX. DAMAGES

9.01 Availability and Assessment

HHSC will be entitled to actual, direct, indirect, incidental, special, and consequential damages resulting from Contractor's failure to comply with any of the terms of the Contract. In some cases, the actual damage to HHSC as a result of Contractor's failure to meet the responsibilities or performance standards of the Contract are difficult or impossible to determine with precise accuracy. Therefore, if provided in the Contract, liquidated damages may be assessed against Contractor for failure to meet any aspect of the Work or responsibilities of the Contractor. HHSC may elect to collect liquidated damages:

(a) Through direct assessment and demand for payment to Contractor; or
(b) By deducting the amounts assessed as liquidated damages against payments owed to Contractor for Work performed. In its sole discretion, HHSC may deduct amounts assessed as liquidated damages as a single lump sum payment or as multiple payments until the full amount payable by the Contractor is received by the HHSC.

9.02 Specific Items of Liability

Contractor bears all risk of loss or damage due to defects in the Work, unfitness or obsolescence of the Work, or the negligence or intentional misconduct of Contractor or Contractor Agents. Contractor will ship all equipment and Software purchased and Third Party Software licensed under the Contract, freight prepaid, FOB HHSC's destination. The method of shipment will be consistent with the nature of the items shipped and applicable hazards of transportation to such items. Regardless of FOB point, Contractor bears all risks of loss, damage, or destruction of the Work, in whole or in part, under the Contract that occurs prior to acceptance by HHSC. After acceptance by HHSC, the risk of loss or damage will be borne by HHSC; however, Contractor remains liable for loss or damage attributable to Contractor's fault or negligence.

Contractor will protect HHSC's real and personal property from damage arising from Contractor or Contractor Agents performance of the Contract, and Contractor will be responsible for any loss, destruction, or damage to HHSC's property that results from or is caused by Contractor or Contractor Agents' negligent or wrongful acts or omissions. Upon the loss of, destruction of, or damage to any property of HHSC, Contractor will notify HHSC thereof and, subject to direction from HHSC or its designee, will take all reasonable steps to protect that property from further damage. Contractor agrees, and will require Contractor Agents, to observe safety measures and proper operating procedures at HHSC sites at all times. Contractor will immediately report to the HHSC any special defect or an unsafe condition it encounters or otherwise learns about.

IN COORDINATION WITH THE INDEMNITY PROVISIONS CONTAINED IN THE UTC, Contractor WILL BE SOLELY RESPONSIBLE FOR ALL COSTS

INCURRED THAT ARE ASSOCIATED WITH INDEMNIFYING THE STATE OF TEXAS OR HHSC WITH RESPECT TO INTELLECTUAL, REAL AND PERSONAL PROPERTY. ADDITIONALLY, HHSC RESERVES THE RIGHT TO APPROVE COUNSEL SELECTED BY Contractor TO DEFEND HHSC OR THE STATE OF TEXAS AS REQUIRED UNDER THIS SECTION.

Article X. ADDITIONAL LICENSE AND OWNERSHIP PROVISIONS

10.01 HHSC Additional Rights

HHSC will have ownership and unlimited rights to use, disclose, duplicate, or publish all information and data developed, derived, documented, or furnished by Contractor under or resulting from the Contract. Such data will include all results, technical information, and materials developed for or obtained by HHSC from Contractor in the performance of the Work. If applicable, Contractor will reproduce and include HHSC's copyright, proprietary notice, or any product identifications provided by Contractor.

10.02 Software and Ownership Rights

In accordance with 45 C.F.R. Part 95.617, all appropriate federal agencies will have a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, translate, or otherwise use, and to authorize others to use for government purposes all Work, materials, Custom Software and modifications thereof, source code, associated documentation designed, developed, or installed with Federal Financial Participation under the Contract, including but not limited to those materials covered by copyright.

Article XI. UNIFORM ICT ACCESSIBILITY CLAUSE

11.01 Applicability

This Section applies to the procurement or development of Information and Communication Technology (ICT) for HHSC, or any changes to HHSC's ICT. This Section also applies if the Contract requires Contractor to perform a service or supply a goods that include ICT that: (i) HHSC employees are required or permitted to access; or (ii) members of the public are required or permitted to access. This Section does not apply to incidental uses of ICT in the performance of a contract, unless the parties agree that the ICT will become property of the state or will be used by HHSC's Client/Recipient after completion of the Contract.

Nothing in this section is intended to prescribe the use of particular designs or technologies or to prevent the use of alternative technologies, provided they result in substantially equivalent or greater access to and use of a product / service.

11.02 Definitions

The legacy term "Electronic and Information Resources" (EIR) and the term "Information and Communication Technology" (ICT) are considered equivalent in meaning for the purpose of applicability of HHSC Uniform Terms and Conditions, policies, accessibility checklists, style guides, contract specifications, and other contract management documents. To the extent that any other of the following definitions conflict with definitions elsewhere in this Contract, the following definitions are applicable to this Section only.

1. **"Accessibility Standards"** refers to the Information and Communication Technology Accessibility Standards and the Web Accessibility Standards/Specifications under the Web Content Accessibility Guidelines version 2.0 Level AA, (WCAG 2.0).

2. **"Information and Communication Technology (ICT)"** is any information technology, equipment, or interconnected system or subsystem of equipment for which the principal function is the creation, conversion, duplication, automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, reception, or broadcast of data or information. Examples of ICT are electronic content, telecommunications products, computers and ancillary equipment, software, information kiosks and transaction machines, videos, IT services, and multifunction office machines which copy, scan, and fax documents.

3. **"Information and Communication Technology Accessibility Standards"** refers to the accessibility standards for information and communication technology contained in the Web Content Accessibility Guidelines version 2.0 Level AA.

4. **"Web Accessibility Standards/Specifications"** refers to the web standards contained in WCAG 2.0 Level AA.

5. **"Products"** means information resources technologies that are, or are related to, ICT.

6. **"Service"** means the act of delivering information or performing a task for employees, clients, or members of the public through a method of access or delivery that uses ICT.

11.03 Accessibility Requirements

Under Texas Government Code Chapter 2054, Subchapter M, and implementing rules of the Texas Department of Information Resources, HHSC must procure Products or Services that comply with the Accessibility Standards when such Products or Services are available in the commercial marketplace or when such Products or Services are developed in response to a procurement solicitation. Accordingly, Contractor must provide ICT and associated Product and/or Service documentation and technical support that comply with the Accessibility Standards.

11.04 Evaluation, Testing and Monitoring

1. HHSC may review, test, evaluate and monitor Contractor's Products, Services and associated documentation and technical support for compliance with the Accessibility Standards. Review, testing, evaluation and monitoring may be conducted before and after the award of a contract. Testing and monitoring may include user acceptance testing.
1. Neither (1) the review, testing (including acceptance testing), evaluation or monitoring of any Product or Service, nor (2) the absence of such review, testing, evaluation or monitoring, will result in a waiver of the State's right to contest the Contractor's assertion of compliance with the Accessibility Standards.

2. Contractor agrees to cooperate fully and provide HHSC and its representatives timely access to Products, Services, documentation, and other items and information needed to conduct such review, evaluation, testing and monitoring.

11.05 Representations and Warranties

1. Contractor represents and warrants that: (i) as of the effective date of the contract, the Products, Services and associated documentation and technical support comply with the Accessibility Standards as they exist at the time of entering the contract, unless and to the extent the Parties otherwise expressly agree in writing; and (ii) if the Products will be in the custody of the state or an HHS agency's client or recipient after the contract expiration or termination, the Products will continue to comply with such Accessibility Standards after the expiration or termination of the contract term, unless HHSC and/or Client/Recipient, as applicable uses the Products in a manner that renders it noncompliant.

2. In the event Contractor should have known, becomes aware, or is notified that the Product and associated documentation and technical support do not comply with the Accessibility Standards, Contractor represents and warrants that it will, in a timely manner and at no cost to HHSC, perform all necessary steps to satisfy the Accessibility Standards, including but not limited to remediation, repair, replacement, and upgrading of the Product, or providing a suitable substitute.

3. Contractor acknowledges and agrees that these representations and warranties are essential inducements on which HHSC relies in awarding this contract.

4. Contractor's representations and warranties under this subsection will survive the termination or expiration of the contract and will remain in full force and effect throughout the useful life of the Product.

11.06 Remedies

1. Pursuant to Texas Government Code Sec. 2054.465, neither Contractor nor any other person has cause of action against HHSC for a claim of a failure to comply with Texas Government Code Chapter 2054, Subchapter M, and rules of the Department of Information Resources.

2. In the event of a breach of Contractor's representations and warranties, Contractor will be liable for direct and consequential damages and any other remedies to which HHSC may be entitled. This remedy is cumulative of any and all other remedies to which HHSC may be entitled under this contract and other applicable law.

Article XII. MISCELLANEOUS PROVISIONS

12.01 Conflicts of Interest

Contractor warrants to the best of its knowledge and belief, except to the extent already disclosed to HHSC, there are no facts or circumstances that could give rise to a Conflict of Interest and further that Contractor or Contractor Agents have no interest and will not acquire any direct or indirect interest that would conflict in any manner or degree with their performance under the Contract. Contractor will, and require Contractor Agents, to establish safeguards to prohibit Contract Agents from using their positions for a purpose that constitutes or presents the appearance of personal or organizational Conflict of Interest, or for personal gain. Contractor and Contractor Agents will operate with complete independence and objectivity without actual, potential or apparent Conflict of Interest with respect to the activities conducted under the Contract.

Contractor agrees that, if after Contractor's execution of the Contract, Contractor discovers or is made aware of a Conflict of Interest, Contractor will immediately and fully disclose such interest in writing to HHSC. In addition, Contractor will promptly and fully disclose any relationship that might be perceived or represented as a conflict after its discovery by Contractor or by HHSC as a potential conflict. HHSC reserves the right to make a final determination regarding the existence of Conflicts of Interest, and Contractor agrees to abide by HHSC's decision.

If HHSC determines that Contractor was aware of a Conflict of Interest and did not disclose the conflict to HHSC, such nondisclosure will be considered a material breach of the Contract. Furthermore, such breach may be submitted to the Office of the Attorney General, Texas Ethics Commission, or appropriate State or federal law enforcement officials for further action.

12.02 Flow Down Provisions

Contractor must include any applicable provisions of the Contract in all subcontracts based on the scope and magnitude of Work to be performed by such Subcontractor. Any necessary terms will be modified appropriately to preserve the State's rights under the Contract.

12.03 Manufacturer's Warranties

Contractor assigns to HHSC all of the manufacturers' warranties and indemnities relating to the Work, including without limitation, Third Party Software, to the extent Contractor is permitted by the manufacturers to make such assignments to HHSC.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit D: HHSC Data Use Agreement (DUA) and Security Privacy Inquiry (SPI)

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

DATA USE AGREEMENT
BETWEEN THE
TEXAS HEALTH AND HUMAN SERVICES SYSTEM AND
CONTRACTOR

This Data Use Agreement ("DUA") is effective as of the date of the Base Contract into which it is incorporated ("Effective Date"), by and between the Texas Health and Human Services System, which includes the Texas Health and Human Services Commission and the Department of State Health Services ("HHS") and Contractor (the "Base Contract").

ARTICLE 1. PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure or transmission of Confidential Information with Contractor, and describe Contractor's rights and obligations with respect to the Confidential Information and the limited purposes for which the Contractor may create, receive, maintain, use, disclose or have access to Confidential Information. This DUA also describes HHS's remedies in the event of Contractor's noncompliance with its obligations under this DUA. This DUA applies to both HHS business_associates, as "business associate" is defined in the Health Insurance Portability and Accountability Act (HIPAA), and contractors who are not business associates, who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of HHS, its programs or clients as described in the Base Contract. As a best practice, HHS requires its contractors to comply with the terms of this DUA to safeguard all types of Confidential Information.

As of the Effective Date of this DUA, if any provision of the Base Contract conflicts with this DUA, this DUA controls.

ARTICLE 2. DEFINITIONS

For the purposes of this DUA, capitalized, underlined terms have the following meanings:

"Authorized Purpose" means the specific purpose or purposes described in the Base Contract for Contractor to fulfill its obligations under the Base Contract, or any other purpose expressly authorized by HHS in writing in advance.

"Authorized User" means a person:

(1) Who is authorized to create, receive, maintain, have access to, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;

(2) For whom Contractor warrants and represents has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and

(3) Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.

"Breach" means an impermissible use or disclosure of electronic or non-electronic sensitive personal information by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of Confidential Information such that the use or disclosure poses a risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Any acquisition, access, use, disclosure or loss of Confidential Information other than as permitted by this DUA shall be presumed to be a Breach

unless Contractor demonstrates, based on a risk assessment, that there is a low probability that the Confidential Information has been compromised.

"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to Contractor or that Contractor may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following:

(1) Education records as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g; 34 C.F.R. Part 99

(2) Federal Tax Information as defined in Internal Revenue Code §6103 and Internal Revenue Service Publication 1075;

(3) Personal Identifying Information (PII) as defined in Texas Business and Commerce Code, Chapter 521;

(4) Protected Health Information (PHI) in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information as defined in 45 C.F.R. §160.103;

(5) Sensitive Personal Information (SPI) as defined in Texas Business and Commerce Code, Chapter 521;

(6) Social Security Administration Data, including, without limitation, Medicaid information means disclosures of information made by the Social Security Administration or the Centers for Medicare and Medicaid Services from a federal system of records for administration of federally funded benefit programs under the Social Security Act, 42 U.S.C., Chapter 7;

(7) All privileged work product;

(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

"Destroy", "Destruction", for Confidential Information, means:

(1) Paper, film, or other hard copy media have been shredded or destroyed such that the Confidential Information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

(2) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization," such that the Confidential Information cannot be retrieved.

"Discover, Discovery" means the first day on which a Breach becomes known to Contractor, or, by exercising reasonable diligence would have been known to Contractor.

"Legally Authorized Representative" of an individual, including as provided in 45 CFR 435.923 (authorized representative); 45 CFR 164.502(g)(1) (personal representative); Tex. Occ. Code § 151.002(6); Tex. H. & S. Code §166.164 (medical power of attorney); and Texas Estates Code § 22.031 (representative).

"Required by Law" means a mandate contained in law that compels an entity to use or disclose Confidential Information that is enforceable in a court of law, including court orders, warrants, subpoenas or investigative demands.

"Subcontractor" means a person who contracts with a prime contractor to work, to supply commodities, or to contribute toward completing work for a governmental entity.

"Workforce" means employees, volunteers, trainees or other persons whose performance of work is under the direct control of a party, whether or not they are paid by that party.

ARTICLE 3. CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION

Section 3.01 Obligations of Contractor Contractor agrees that:

(A) With respect to PHI, Contractor shall:

(1) Make PHI available in a designated record set if requested by HHS, if Contractor maintains PHI in a designated record set, as defined in HIPAA.

(2) Provide to HHS data aggregation services related to the healthcare operations Contractor performs for HHS pursuant to the Base Contract, if requested by HHS, if Contractor provides data aggregation services as defined in HIPAA.

(3) Provide access to PHI to an individual who is requesting his or her own PHI, or such individual's Legally Authorized Representative, in compliance with the requirements of HIPAA.

(4) Make PHI available to HHS for amendment, and incorporate any amendments to PHI that HHS directs, in compliance with HIPAA.

(5) Document and make available to HHS, an accounting of disclosures in compliance with the requirements of HIPAA.

(6) If Contractor receives a request for access, amendment or accounting of PHI by any individual, promptly forward the request to HHS or, if forwarding the request would violate HIPAA, promptly notify HHS of the request and of Contractor's response. HHS will respond to all such requests, unless Contractor is Required by Law to respond or HHS has given prior written consent for Contractor to respond to and account for all such requests.

(B) With respect to ALL Confidential Information, Contractor shall:

(1) Exercise reasonable care and no less than the same degree of care Contractor uses to protect its own confidential, proprietary and trade secret information to prevent Confidential Information from being used in a manner that is not expressly an Authorized Purpose or as Required by Law. Contractor will access, create, maintain, receive, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses.

(2) Establish, implement and maintain appropriate procedural, administrative, physical and technical safeguards to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, in accordance with applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as Contractor has such Confidential Information in its actual or constructive possession.

(3) Implement, update as necessary, and document privacy, security and Breach notice policies and procedures and an incident response plan to address a Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Base Contract. Contractor shall produce, within three business days of a request by HHS, copies of its policies and procedures and records relating to the use or disclosure of Confidential Information.

(4) Obtain HHS's prior written consent to disclose or allow access to any portion of the Confidential Information to any person, other than Authorized Users, Workforce or Subcontractors of Contractor who have completed training in confidentiality, privacy, security and the importance of promptly reporting any Breach to Contractor's management and as permitted in Section 3.01(A)(3), above. Contractor shall produce evidence of completed training to HHS upon request. HHS, at its election, may assist Contractor in training and education on specific or unique HHS processes, systems and/or requirements.

(5) Establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Base Contract or applicable law. Contractor shall maintain evidence of sanctions and produce it to HHS upon request.

(6) Obtain prior written approval of HHS, to disclose or provide access to any Confidential Information on the basis that such act is Required by Law, so that HHS may have the opportunity to object to the disclosure or access and seek appropriate relief. If HHS objects to such disclosure or access, Contractor shall refrain from disclosing or providing access to the Confidential Information until HHS has exhausted all alternatives for relief.

(7) Certify that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose and that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. Contractor and its Subcontractors shall maintain at all times an updated, complete, accurate list of Authorized Users and supply it to HHS upon request.

(8) Provide, and shall cause its Subcontractors and agents to provide, to HHS periodic written confirmation of compliance with controls and the terms and conditions of this DUA.

(9) Return to HHS or Destroy, at HHS's election and at Contractor's expense, all Confidential Information received from HHS or created or maintained by Contractor or any of Contractor's agents or Subcontractors on HHS's behalf upon the termination or expiration of this DUA, if reasonably feasible and permitted by law. Contractor shall certify in writing to HHS that all such Confidential Information has been Destroyed or returned to HHS, and that Contractor and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, Contractor acknowledges and agrees that it may not Destroy any Confidential Information if federal or state law, or HHS record retention policy or a litigation hold notice prohibits such Destruction. If such return or Destruction is not reasonably feasible, or is impermissible by law, Contractor shall immediately notify HHS of the reasons such return or Destruction is not feasible, and agree to extend the protections of this DUA to the Confidential Information for as long as Contractor maintains such Confidential Information.

(10) Complete and return with the Base Contract to HHS, attached as Attachment 2 to this DUA, the HHS Security and Privacy Initial Inquiry (SPI) at ***https://hhs.texas.gov/lawsregulations/forms/miscellaneous/hhs-information-security-privacy-initial-inquiry-spi.*** The SPI identifies basic privacy and security controls with which Contractor must comply to protect Confidential Information. Contractor shall comply with periodic security controls compliance assessment and monitoring by HHS as required by state and federal law, based on the type of Confidential

Information Contractor creates, receives, maintains, uses, discloses or has access to and the Authorized Purpose and level of risk. Contractor's security controls shall be based on the National Institute of Standards and Technology (NIST) Special Publication 800-53. Contractor shall update its security controls assessment whenever there are significant changes in security controls for HHS Confidential Information and shall provide the updated document to HHS. HHS also reserves the right to request updates as needed to satisfy state and federal monitoring requirements.

(11) Comply with the HHS Acceptable Use Policy (AUP) and require each Subcontractor and Workforce member who has direct access to HHS Information Resources, as defined in the AUP, to execute an HHS Acceptable Use Agreement.

(12) Only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. A secure transmission of electronic Confidential Information *in motion* includes secure File Transfer Protocol (SFTP) or encryption at an appropriate level as required by rule, regulation or law. Confidential Information *at rest* requires encryption unless there is adequate administrative, technical, and physical security as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information shall be through secure systems. Contractor shall provide proof of system, media or device security and/or encryption to HHS no later than 48 hours after HHS's written request in response to a compliance investigation, audit, or the Discovery of a Breach. HHS may also request production of proof of security at other times as necessary to satisfy state and federal monitoring requirements. Deidentification of Confidential Information in accordance with HIPAA de-identification standards is deemed secure.

(13) Designate and identify a person or persons, as Privacy Official and Information Security Official, each of whom is authorized to act on behalf of Contractor and is responsible for the development and implementation of the privacy and security requirements in this DUA. Contractor shall provide name and current address, phone number and e-mail address for such designated officials to HHS upon execution of this DUA and prior to any change. Upon written notice from HHS, Contractor shall promptly remove and replace such official(s) if such official(s) is not performing the required functions.

(14) Make available to HHS any information HHS requires to fulfill HHS's obligations to provide access to, or copies of, Confidential Information in accordance with applicable laws, regulations or demands of a regulatory authority relating to Confidential Information. Contractor shall provide such information in a time and manner reasonably agreed upon or as designated by the applicable law or regulatory authority.

(15) Comply with the following laws and standards ***if applicable to the type of Confidential Information and Contractor's Authorized Purpose***:

- Title 1, Part 10, Chapter 202, Subchapter B, Texas Administrative Code;
- The Privacy Act of 1974;
- OMB Memorandum 17-12;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;

- National Institute of Standards and Technology (NIST) Special Publication 800-66 Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI;
- Family Educational Rights and Privacy Act
- Any other State or Federal law, regulation, or administrative rule relating to the specific HHS program area that Contractor supports on behalf of HHS.

(16) Be permitted to use or disclose Confidential Information for the proper management and administration of Contractor or to carry out Contractor's legal responsibilities, except as otherwise limited by this DUA, the Base Contract, or law applicable to the Confidential Information, if:

(a) Disclosure is Required by Law;

(b) Contractor obtains reasonable assurances from the person to whom the information is disclosed that the person shall:

1. Maintain the confidentiality of the Confidential Information in accordance with this DUA;

2. Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the person; and

3. Notify Contractor in accordance with Section 4.01 of a Breach of Confidential Information that the person Discovers or should have Discovered with the exercise of reasonable diligence.

(C) With respect to ALL Confidential Information, Contractor shall NOT:

(1) Attempt to re-identify or further identify Confidential Information that has been deidentified, or attempt to contact any persons whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from HHS.

(2) Engage in prohibited marketing or sale of Confidential Information.

(3) Permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of HHS without requiring that Subcontractor first execute either the Form Subcontractor Agreement, Attachment 1, or Contractor's own Subcontractor agreement that ensures that the Subcontractor shall comply with the same safeguards and restrictions contained in this DUA for Confidential Information. Contractor is directly responsible for its Subcontractors' compliance with, and enforcement of, this DUA.

ARTICLE 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

Section 4.01. Cooperation and Financial Responsibility.

(A) Contractor shall, at Contractor's expense, cooperate fully with HHS in investigating, mitigating to the extent practicable, and issuing notifications as directed by HHS, for any Breach of Confidential Information.

(B) Contractor shall make Confidential Information in Contractor's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach.

(C) Contractor's obligation begins at the Discovery of a Breach and continues as long as related activity continues, until all effects of the Breach are mitigated to HHS's satisfaction (the "incident response period").

Section 4.02. Initial Breach Notice.

For federal information ***obtained from a federal system of records***, including Federal Tax Information and Social Security Administration Data (which includes Medicaid and other governmental benefit program Confidential Information), Contractor shall notify HHS of the Breach within the first consecutive clock hour of Discovery. The Base Contract shall specify whether Confidential Information is obtained from a federal system of records. For all other types of Confidential Information Contractor shall notify HHS of the Breach not more than 24 hours after Discovery, ***or in a timeframe otherwise approved by HHS in writing.*** Contractor shall initially report to HHS's Privacy and Security Officers via email at: privacy@HHSC.state.tx.us and to the HHS division responsible for the Base Contract. Contractor shall report all information reasonably available to Contractor about the Breach.

Contractor shall provide contact information to HHS for Contractor's single point of contact who will communicate with HHS both on and off business hours during the incident response period.

Section 4.03 Third Business Day Notice: No later than 5 p.m. on the third business day after Discovery, or a time within which Discovery reasonably should have been made by Contractor of a Breach of Confidential Information, Contractor shall provide written notification to HHS of all reasonably available information about the Breach, and Contractor's investigation, including, to the extent known to Contractor***:***
a. The date the Breach occurred;

b. The date of Contractor's and, if applicable, Subcontractor's Discovery;

c. A brief description of the Breach, including how it occurred and who is responsible (or hypotheses, if not yet determined);

d. A brief description of Contractor's investigation and the status of the investigation;

e. A description of the types and amount of Confidential Information involved;

f. Identification of and number of all individuals reasonably believed to be affected, including first and last name of the individual and if applicable, the Legally authorized representative, last known address, age, telephone number, and email address if it is a preferred contact method;

g. Contractor's initial risk assessment of the Breach demonstrating whether individual or other notices are required by applicable law or this DUA for HHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;

h. Contractor's recommendation for HHS's approval as to the steps individuals and/or Contractor on behalf of individuals, should take to protect the individuals from potential harm, including Contractor's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;

i. The steps Contractor has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);

j. The steps Contractor has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Breach;

k. Identify, describe or estimate of the persons, Workforce, Subcontractor, or individuals and any law enforcement that may be involved in the Breach;

l. A reasonable schedule for Contractor to provide regular updates regarding response to the Breach, but no less than every three (3) business days, or as otherwise directed by HHS in writing, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

m. Any reasonably available, pertinent information, documents or reports related to a Breach that HHS requests following Discovery.

Section 4.04. Investigation, Response and Mitigation.

(A) Contractor shall immediately conduct a full and complete investigation, respond to the Breach, commit necessary and appropriate staff and resources to expeditiously respond, and report as required to HHS for incident response purposes and for purposes of HHS's compliance with report and notification requirements, to the satisfaction of HHS.

(B) Contractor shall complete or participate in a risk assessment as directed by HHS following a Breach, and provide the final assessment, corrective actions and mitigations to HHS for review and approval.

(C) Contractor shall fully cooperate with HHS to respond to inquiries and/or proceedings by state and federal authorities, persons and/or individuals about the Breach.

(D) Contractor shall fully cooperate with HHS's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such Breach, or to recover or protect any Confidential Information, including complying with reasonable corrective action or measures, as specified by HHS in a Corrective Action Plan if directed by HHS under the Base Contract.

Section 4.05. Breach Notification to Individuals and Reporting to Authorities.

(A) HHS may direct Contractor to provide Breach notification to individuals, regulators or third-parties, as specified by HHS following a Breach.

(B) Contractor must comply with all applicable legal and regulatory requirements in the time, manner and content of any notification to individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in Contractor's name and on Contractor's letterhead, unless otherwise directed by HHS, and will contain contact information, including the name and title of Contractor's representative, an email address and a toll-free telephone number, for the individual to obtain additional information.

(C) Contractor shall provide HHS with draft notifications for HHS approval prior to distribution and copies of distributed and approved communications.

(D) Contractor shall have the burden of demonstrating to the satisfaction of HHS that any required notification was timely made. If there are delays outside of Contractor's control, Contractor shall provide written documentation to HHS of the reasons for the delay.

(E) If HHS directs Contractor to provide notifications, HHS shall, in the time and manner reasonably requested by Contractor, cooperate and assist with Contractor's information requests in order to make such notifications.

ARTICLE 5. GENERAL PROVISIONS

Section 5.01 Ownership of Confidential Information

Contractor acknowledges and agrees that the Confidential Information is and shall remain the property of HHS. Contractor agrees it acquires no title or rights to the Confidential Information.

Section 5.02 HHS Commitment and Obligations

HHS will not request Contractor to create, maintain, transmit, use or disclose PHI in any manner that would not be permissible under applicable law if done by HHS.

Section 5.03 HHS Right to Inspection

At any time upon reasonable notice to Contractor, or if HHS determines that Contractor has violated this DUA, HHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of Contractor to monitor compliance with this DUA. For purposes of this subsection, HHS's agent(s) include, without limitation, the HHS Office of the Inspector General, the Office of the Attorney General of Texas, the State Auditor's Office, outside consultants, legal counsel or other designee.

Section 5.04 Term; Termination of DUA; Survival

This DUA will be effective on the date on which Contractor executes the Base Contract, and will terminate upon termination of the Base Contract and as set forth herein. If the Base Contract is extended, this DUA is extended to run concurrent with the Base Contract.

(A) If HHS determines that Contractor has violated a material term of this DUA; HHS may in its sole discretion:

(1) Exercise any of its rights including but not limited to reports, access and inspection under this DUA and/or the Base Contract; or

(2) Require Contractor to submit to a corrective action plan, including a plan for monitoring and plan for reporting as HHS may determine necessary to maintain compliance with this DUA; or

(3) Provide Contractor with a reasonable period to cure the violation as determined by HHS; or

(4) Terminate the DUA and Base Contract immediately, and seek relief in a court of competent jurisdiction in Travis County, Texas.

Before exercising any of these options, HHS will provide written notice to Contractor describing the violation and the action it intends to take.

(B) If neither termination nor cure is feasible, HHS shall report the violation to the applicable regulatory authorities.

(C) The duties of Contractor or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to HHS, as required by this DUA.

Section 5.05 Injunctive Relief

(A) Contractor acknowledges and agrees that HHS may suffer irreparable injury if Contractor or its Subcontractor fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

(B) Contractor further agrees that monetary damages may be inadequate to compensate HHS for Contractor's or its Subcontractor's failure to comply. Accordingly, Contractor agrees that HHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

Section 5.06 Indemnification

Contractor shall indemnify, defend and hold harmless HHS and its respective Executive Commissioner, employees, Subcontractors, agents (including other state agencies acting on behalf of HHS) or other members of HHS' Workforce (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this DUA or from any acts or omissions related to this DUA by Contractor or its employees, directors, officers, Subcontractors, or agents or other members of Contractor's Workforce. The duty to indemnify, defend and hold harmless is independent of the duty to insure. Upon demand, Contractor shall reimburse HHS for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including costs of required notices, investigation, and mitigation of a Breach, fines or penalties imposed on an Indemnified Party by a regulatory authority, and reasonable attorneys' fees) which may be imposed upon any Indemnified Party to the extent caused by and which results from the Contractor's failure to meet any of its obligations under this DUA. Contractor's obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this DUA.

Section 5.07 Insurance

(A) In addition to any insurance required in the Base Contract, at HHS's option, HHS may require Contractor to maintain, at its expense, the special and/or custom first- and third-party insurance coverages, including without limitation data breach, cyber liability, crime theft and notification expense coverages, with policy limits sufficient to cover any liability arising under this DUA, naming the State of Texas, acting through HHS, as an additional named insured and loss payee, with primary and noncontributory status.

(B) Contractor shall provide HHS with written proof that required insurance coverage is in effect, at the request of HHS.

Section 5.08 Entirety of the Contract

This DUA is incorporated by reference into the Base Contract and, together with the Base Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced.

Section 5.09 Automatic Amendment and Interpretation

Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on HHS and/or Contractor remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits HHS and Contractor to comply with laws applicable to Confidential Information.

Section 5.10 Notices; Requests for Approval

All notices and requests for approval related to this DUA must be directed to the HHS Chief Privacy Officer at privacy@hhsc.state.tx.us.

ATTACHMENT 1. SUBCONTRACTOR AGREEMENT FORM

HHS CONTRACT NUMBER _____

The DUA between HHS and Contractor establishes the permitted and required uses and disclosures of Confidential Information by Contractor.

Contractor has subcontracted with_____ (Subcontractor) for performance of duties on behalf of CONTRACTOR which are subject to the DUA. Subcontractor acknowledges, understands and agrees to be bound by the same terms and conditions applicable to Contractor under the DUA, incorporated by reference in this Agreement, with respect to HHS Confidential Information. Contractor and Subcontractor agree that HHS is a third-party beneficiary to applicable provisions of the subcontract.

HHS has the right, but not the obligation, to review or approve the terms and conditions of the subcontract by virtue of this Subcontractor Agreement Form.

Contractor and Subcontractor assure HHS that any Breach as defined by the DUA that Subcontractor Discovers shall be reported to HHS by Contractor in the time, manner and content required by the DUA.

If Contractor knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by Subcontractor that constitutes a material breach or violation of the DUA or the Subcontractor's obligations, Contractor shall:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract or arrangement with Subcontractor, if feasible;
3. Notify HHS immediately upon Discovery of the pattern of activity or practice of Subcontractor that constitutes a material breach or violation of the DUA and keep HHS reasonably and regularly informed about steps Contractor is taking to cure or end the violation or terminate Subcontractor's contract or arrangement.

This Subcontractor Agreement Form is executed by the parties in their capacities indicated below.

CONTRACTOR	SUBCONTRACTOR
BY: _____	_____
	BY:
NAME: _____	NAME:_____
TITLE: _____	TITLE:_____
DATE _____, 201 . __	DATE:_____

Texas HHS System - Data Use Agreement - Attachment 2
SECURITY AND PRIVACY INQUIRY (SPI)

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A: APPLICANT/BIDDER INFORMATION (To be completed by Applicant/Bidder)

1. Does the applicant/bidder access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.)? **IF NO, STOP. THE SPI FORM IS NOT REQUIRED.**	○ Yes ○ No
2. Entity or Applicant/Bidder Legal Name	Legal Name: Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): Procurement/Contract#: Address: City: State: ZIP: Telephone #: Email Address:
3. Number of Employees, at all locations, in Applicant/Bidder's Workforce "Workforce" means all employees, volunteers, trainees, and other Persons whose conduct is under the direct control of Applicant/Bidder, whether or not they are paid by Applicant/ Bidder. If Applicant/Bidder is a sole proprietor, the workforce may be only one employee.	Total Employees:
4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")	Total Subcontractors:
5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder (Privacy and Security Official may be the same person.)	**A. Security Official:** Legal Name: Address: City: State: ZIP: Telephone #: Email Address:
	B. Privacy Official: Legal Name: Address: City: State: ZIP: Telephone #: Email Address:

6. **Type(s) of Texas HHS Confidential Information the Applicant/Bidder will create, receive, maintain, use, disclose or have access to: (Check all that apply)** • *Health Insurance Portability and Accountability Act (HIPAA) data* • *Criminal Justice Information Services (CJIS) data* • *Internal Revenue Service Federal Tax Information (IRS FTI) data* • *Centers for Medicare & Medicaid Services (CMS)* • *Social Security Administration (SSA)* • *Personally Identifiable Information (PII)*	HIPAA ☐	CJIS ☐	IRS FTI ☐	CMS ☐	SSA ☐	PII ☐
	Other (Please List)					

7. **Number of Storage Devices for Texas HHS Confidential Information (as defined in the Texas HHS System Data Use Agreement (DUA))** Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.	Total # (Sum a-d) 0
a. Devices. Number of personal user computers, devices or drives, including mobile devices and mobile drives.	
b. Servers. Number of Servers that are not in a data center or using Cloud Services.	
c. Cloud Services. Number of Cloud Services in use.	
d. Data Centers. Number of Data Centers in use.	
8. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year:	Select Option (a-d)
a. 499 individuals or less **b.** 500 to 999 individuals **c.** 1,000 to 99,999 individuals **d.** 100,000 individuals or more	○ a. ○ b. ○ c. ○ d.
9. HIPAA Business Associate Agreement	
a. Will Applicant/Bidder use, disclose, create, receive, transmit or maintain protected health information on behalf of a HIPAA-covered Texas HHS agency for a HIPAA-covered function?	○ Yes ○ No
b. Does Applicant/Bidder have a Privacy Notice prominently displayed on a Webpage or a Public Office of Applicant/Bidder's business open to or that serves the public? (This is a HIPAA requirement. Answer "N/A" if not applicable, such as for agencies not covered by HIPAA.)	○ Yes ○ No ○ N/A
Action Plan for Compliance with a Timeline:	Compliance Date:
10. Subcontractors. If the Applicant/Bidder responded "0" to Question 4 (indicating no subcontractors), check "N/A" for both 'a.' and 'b.'	
a. Does Applicant/Bidder require subcontractors to execute the DUA Attachment 1 Subcontractor Agreement Form?	○ Yes ○ No ○ N/A
Action Plan for Compliance with a Timeline:	Compliance Date:

b. Will Applicant/Bidder agree to require subcontractors who will access Confidential Information to comply with the terms of the DUA, not disclose any Confidential Information to them until they have agreed in writing to the same safeguards and to discontinue their access to the Confidential Information if they fail to comply?	○ Yes ○ No ○ N/A
Action Plan for Compliance with a Timeline:	Compliance Date:
11. Does Applicant/Bidder have any **Optional Insurance** currently in place? Optional Insurance provides coverage for: (1) Network Security and Privacy; (2) Data Breach; (3) Cyber Liability (lost data, lost use or delay/suspension in business, denial of service with e-business, the Internet, networks and informational assets, such as privacy, intellectual property, virus transmission, extortion, sabotage or web activities); (4) Electronic Media Liability; (5) Crime/Theft; (6) Advertising Injury and Personal Injury Liability; and (7) Crisis Management and Notification Expense Coverage.	○ Yes ○ No ○ N/A

SECTION B: PRIVACY RISK ANALYSIS AND ASSESSMENT (To be completed by Applicant/Bidder)	
For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.	
1. Written Policies & Procedures. Does Applicant/Bidder have current written privacy and security policies and procedures that, at a minimum:	**Yes or No**
a. Does Applicant/Bidder have current written privacy and security policies and procedures that identify Authorized Users and Authorized Purposes (as defined in the DUA) relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
b. Does Applicant/Bidder have current written privacy and security policies and procedures that require Applicant/Bidder and its Workforce to comply with the applicable provisions of HIPAA and other laws referenced in the DUA, relating to creation, receipt, maintenance, use, disclosure, access or transmission of Texas HHS Confidential Information on behalf of a Texas HHS agency?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
c. Does Applicant/Bidder have current written privacy and security policies and procedures that limit use or disclosure of Texas HHS Confidential Information to the minimum that is necessary to fulfill the Authorized Purposes?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
d. Does Applicant/Bidder have current written privacy and security policies and procedures that respond to an actual or suspected breach of Texas HHS Confidential Information, to include at a minimum (if any responses are "No" check "No" for all three): i. Immediate breach notification to the Texas HHS agency, regulatory authorities, and other required Individuals or Authorities, in accordance with Article 4 of the DUA; ii. Following a documented breach response plan, in accordance with the DUA and applicable law; & iii. Notifying Individuals and Reporting Authorities whose Texas HHS Confidential Information has been breached, as directed by the Texas HHS agency?	○ Yes ○ No

Action Plan for Compliance with a Timeline:	Compliance Date:
e. Does Applicant/Bidder have current written privacy and security policies and procedures that conduct annual workforce training and monitoring for and correction of any training delinquencies?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
f. Does Applicant/Bidder have current written privacy and security policies and procedures that permit or deny individual rights of access, and amendment or correction, when appropriate?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
g. Does Applicant/Bidder have current written privacy and security policies and procedures that permit only Authorized Users with up-to-date privacy and security training, and with a reasonable and demonstrable need to use, disclose, create, receive, maintain, access or transmit the Texas HHS Confidential Information, to carry out an obligation under the DUA for an Authorized Purpose, unless otherwise approved in writing by a Texas HHS agency?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
h. Does Applicant/Bidder have current written privacy and security policies and procedures that establish, implement and maintain proof of appropriate sanctions against any Workforce or Subcontractors who fail to comply with an Authorized Purpose or who is not an Authorized User, and used or disclosed Texas HHS Confidential Information in violation of the DUA, the Base Contract or applicable law?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
i. Does Applicant/Bidder have current written privacy and security policies and procedures that require updates to policies, procedures and plans following major changes with use or disclosure of Texas HHS Confidential Information within 60 days of identification of a need for update?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

j. Does Applicant/Bidder have current written privacy and security policies and procedures that restrict permissions or attempts to re-identify or further identify de-identified Texas HHS Confidential Information, or attempt to contact any Individuals whose records are contained in the Texas HHS Confidential Information, except for an Authorized Purpose, without express written authorization from a Texas HHS agency or as expressly permitted by the Base Contract?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
k. If Applicant/Bidder intends to use, disclose, create, maintain, store or transmit Texas HHS Confidential Information outside of the United States, will Applicant/Bidder obtain the express prior written permission from the Texas HHS agency and comply with the Texas HHS agency conditions for safeguarding offshore Texas HHS Confidential Information?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
l. Does Applicant/Bidder have current written privacy and security policies and procedures that require cooperation with Texas HHS agencies' or federal regulatory inspections, audits or investigations related to compliance with the DUA or applicable law?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
m. Does Applicant/Bidder have current written privacy and security policies and procedures that require appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
n. Does Applicant/Bidder have current written privacy and security policies and procedures that prohibit disclosure of Applicant/Bidder's work product done on behalf of Texas HHS pursuant to the DUA, or to publish Texas HHS Confidential Information without express prior approval of the Texas HHS agency?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder have a current Workforce training program? Training of Workforce must occur at least once every year, and within 30 days of date of hiring a new Workforce member who will handle Texas HHS Confidential Information. Training must include: (1) privacy and security policies, procedures, plans and applicable requirements for handling Texas HHS Confidential Information, (2) a requirement to complete training before access is given to Texas HHS Confidential Information, and (3) written proof of training and a procedure for monitoring timely completion of training.	○ Yes ○ No

Action Plan for Compliance with a Timeline:	Compliance Date:
3. Does Applicant/Bidder have Privacy Safeguards to protect Texas HHS Confidential Information in oral, paper and/or electronic form? "Privacy Safeguards" means protection of Texas HHS Confidential Information by establishing, implementing and maintaining required Administrative, Physical and Technical policies, procedures, processes and controls, required by the DUA, HIPAA (45 CFR 164.530), Social Security Administration, Medicaid and laws, rules or regulations, as applicable. Administrative safeguards include administrative protections, policies and procedures for matters such as training, provision of access, termination, and review of safeguards, incident management, disaster recovery plans, and contract provisions. Technical safeguards include technical protections, policies and procedures, such as passwords, logging, emergencies, how paper is faxed or mailed, and electronic protections such as encryption of data. Physical safeguards include physical protections, policies and procedures, such as locks, keys, physical access, physical storage and trash.	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
4. Does Applicant/Bidder and all subcontractors (if applicable) maintain a current list of Authorized Users who have access to Texas HHS Confidential Information, whether oral, written or electronic?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
5. Does Applicant/Bidder and all subcontractors (if applicable) monitor for and remove terminated employees or those no longer authorized to handle Texas HHS Confidential Information from the list of Authorized Users?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

SECTION C: SECURITY RISK ANALYSIS AND ASSESSMENT (to be completed by Applicant/Bidder)	
This section is about your electronic system. If your business DOES NOT store, access, or transmit Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.) select the box to the right, and "YES" will be entered for all questions in this section.	**No Electronic Systems** ☐
For any questions answered "No," an Action Plan for Compliance with a Timeline must be documented in the designated area below the question. The timeline for compliance with HIPAA-related items is 30 calendar days, PII-related items is 90 calendar days.	
1. Does the Applicant/Bidder ensure that services which access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information are maintained **IN** the United States (no offshoring) unless **ALL** of the following requirements are met? **a.** The data is encrypted with FIPS 140-2 validated encryption **b.** The offshore provider does not have access to the encryption keys **c.** The Applicant/Bidder maintains the encryption key within the United States **d.** The Application/Bidder has obtained the express prior written permission of the Texas HHS agency *For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips*	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
2. Does Applicant/Bidder utilize an IT security-knowledgeable person or company to maintain or oversee the configurations of Applicant/Bidder's computing systems and devices?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
3. Does Applicant/Bidder monitor and manage access to Texas HHS Confidential Information (e.g., a formal process exists for granting access and validating the need for users to access Texas HHS Confidential Information, and access is limited to Authorized Users)?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
4. Does Applicant/Bidder a) have a system for changing default passwords, b) require user password changes at least every 90 calendar days, and c) prohibit the creation of weak passwords (e.g., require a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numerals, where possible) for all computer systems that access or store Texas HHS Confidential Information. **If yes, upon request must provide evidence such as a screen shot or a system report.**	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

5. Does each member of Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information have a unique user name (account) and private password?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
6. Does Applicant/Bidder lock the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store Texas HHS Confidential Information?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
7. Does Applicant/Bidder secure, manage and encrypt remote access (including wireless access) to computer systems containing Texas HHS Confidential Information? (e.g., a formal process exists for granting access and validating the need for users to remotely access Texas HHS Confidential Information, and remote access is limited to Authorized Users). *Encryption is required for all Texas HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
8. Does Applicant/Bidder implement computer security configurations or settings for all computers and systems that access or store Texas HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
9. Does Applicant/Bidder secure physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.)?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

10. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information that is *transmitted* over a public network (e.g., the Internet, WiFi, etc.)? **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
11. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information *stored* on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)? **If yes, upon request must provide evidence such as a screen shot or a system report.** *Encryption is required for all Texas HHS Confidential Information. Additionally, **FIPS 140-2** validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.* *For more information regarding FIPS 140-2 encryption products, please refer to:* *http://csrc.nist.gov/publications/fips*	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
12. Does Applicant/Bidder require Workforce members to formally acknowledge rules outlining their responsibilities for protecting Texas HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
14. Does Applicant/Bidder prohibit the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information with a subcontractor (e.g., cloud services, social media, etc.) unless Texas HHS has approved the subcontractor agreement which must include compliance and liability clauses with the same requirements as the Applicant/Bidder?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

15. Does Applicant/Bidder keep current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
16. Do Applicant/Bidder's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
17. Does the Applicant/Bidder review system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
18. Notwithstanding records retention requirements, does Applicant/Bidder's disposal processes for Texas HHS Confidential Information ensure that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable?	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:
19. Does the Applicant/Bidder ensure that all public facing websites and mobile applications containing Texas HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516; including requirements for implementing vulnerability and penetration testing and addressing identified vulnerabilities? *For more information regarding TGC, Section 2054.516 DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS, please refer to: https://legiscan.com/TX/text/HB8/2017*	○ Yes ○ No
Action Plan for Compliance with a Timeline:	Compliance Date:

SECTION D: SIGNATURE AND SUBMISSION (to be completed by Applicant/Bidder)

Please sign the form digitally, if possible. If you can't, provide a handwritten signature.

1. I certify that all of the information provided in this form is truthful and correct to the best of my knowledge. If I learn that any such information was not correct, I agree to notify Texas HHS of this immediately.

2. Signature	**3.** Title	**4.** Date:

To **submit** the completed, signed form:

- Email the form as an attachment to the appropriate Texas HHS Contract Manager(s).

Section E: To Be Completed by Texas HHS Agency Staff:

Agency(s): HHSC: ☐ DFPS: ☐ DSHS: ☐	Requesting Department(s):
Legal Entity Tax Identification Number (TIN) (Last four Only):	PO/Contract(s) #:

Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:
Contract Manager:	Contract Manager Email Address:	Contract Manager Telephone #:

INSTRUCTIONS FOR COMPLETING THE SECURITY AND PRIVACY INQUIRY (SPI)

Below are instructions for Applicants, Bidders and Contractors for Texas Health and Human Services requiring the Attachment 2, Security and Privacy Inquiry (SPI) to the Data Use Agreement (DUA). Instruction item numbers below correspond to sections on the SPI form.

If you are a bidder for a new procurement/contract, in order to participate in the bidding process, you must have corrected any "No" responses (except A9a) prior to the contract award date. If you are an applicant for an open enrollment, you must have corrected any "No" answers (except A9a and A11) prior to performing any work on behalf of any Texas HHS agency.

For any questions answered "No" (except A9a and A11), an *Action Plan for Compliance with a Timeline* must be documented in the designated area below the question. The timeline for compliance with HIPAA-related requirements for safeguarding Protected Health Information is 30 calendar days from the date this form is signed. Compliance with requirements related to other types of Confidential Information must be confirmed within 90 calendar days from the date the form is signed.

SECTION A. APPLICANT /BIDDER INFORMATION

Item #1. *Only contractors that access, transmit, store, and/or maintain Texas HHS Confidential Information will complete and email this form as an attachment to the appropriate Texas HHS Contract Manager.*

Item #2. Entity or Applicant/Bidder Legal Name. *Provide the legal name of the business (the name used for legal purposes, like filing a federal or state tax form on behalf of the business, and is not a trade or assumed named "dba"), the legal tax identification number (last four numbers only) of the entity or applicant/bidder, the address of the corporate or main branch of the business, the telephone number where the business can be contacted regarding questions related to the information on this form and the website of the business, if a website exists.*

Item #3. Number of Employees, at all locations, in Applicant/Bidder's workforce. *Provide the total number of individuals, including volunteers, subcontractors, trainees, and other persons who work for the business. If you are the only employee, please answer "1."*

Item #4. Number of Subcontractors. *Provide the total number of subcontractors working for the business. If you have none, please answer "0" zero.*

Item #5. Number of unduplicated individuals for whom Applicant/Bidder reasonably expects to handle HHS Confidential Information during one year. *Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Texas HHS Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.*

Item #5. Name of Information Technology Security Official and Name of Privacy Official for Applicant/Bidder. *As with all other fields on the SPI, this is a required field. This may be the same person and the owner of the business if such person has the security and privacy knowledge that is required to implement the requirements of the DUA and respond to questions related to the SPI. In 4.A. provide the name, address, telephone number, and email address of the person whom you have designated to answer any security questions found in Section C and in 4.B. provide this information for the person whom you have designated as the person to answer any privacy questions found in Section B. The business may contract out for this expertise; however, designated individual(s) must have knowledge of the business's devices, systems and methods for use, disclosure, creation, receipt, transmission and maintenance of Texas HHS Confidential Information and be willing to be the point of contact for privacy and security questions.*

Item #6. Type(s) of HHS Confidential Information the Entity or Applicant/Bidder Will Create, Receive, Maintain, Use, Disclose or Have Access to: *Provide a complete listing of all Texas HHS Confidential Information that the Contractor will create, receive, maintain, use, disclose or have access to. The DUA section Article 2, Definitions, defines Texas HHS Confidential Information as:*

> *"Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR or that CONTRACTOR may create, receive, maintain, use, disclose or have access to on behalf of Texas HHS that consists of or includes any or all of the following:*
>
> *(1) Client Information;*
> *(2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information;*
> *(3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521;*

(4) Federal Tax Information;
(5) Personally Identifiable Information;
(6) Social Security Administration Data, including, without limitation, Medicaid information;
(7) All privileged work product;
(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.

Definitions for the following types of confidential information can be found the following sites:

- *Health Insurance Portability and Accountability Act (HIPAA) - http://www.hhs.gov/hipaa/index.html*
- *Criminal Justice Information Services (CJIS) - https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center*
- *Internal Revenue Service Federal Tax Information (IRS FTI) - https://www.irs.gov/pub/irs-pdf/p1075.pdf*
- *Centers for Medicare & Medicaid Services (CMS) - https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Guidance.html*
- *Social Security Administration (SSA) - https://www.ssa.gov/regulations/*
- *Personally Identifiable Information (PII) - http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf*

Item #7. Number of Storage devices for Texas HHS Confidential Information. *The total number of devices is automatically calculated by exiting the fields in lines a - d. Use the <Tab> key when exiting the field to prompt calculation, if it doesn't otherwise sum correctly.*

- ***Item 7a. Devices****. Provide the number of personal user computers, devices, and drives (including mobile devices, laptops, USB drives, and external drives) on which your business stores or will store Texas HHS Confidential Information.*
- ***Item 7b. Servers****. Provide the number of servers not housed in a data center or "in the cloud," on which Texas HHS Confidential Information is stored or will be stored. A server is a dedicated computer that provides data or services to other computers. It may provide services or data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. If none, answer "0" (zero).*
- ***Item 7c. Cloud Services****. Provide the number of cloud services to which Texas HHS Confidential Information is stored. Cloud Services involve using a network of remote servers hosted on the Internet to store, manage, and process data, rather than on a local server or a personal computer. If none, answer "0" (zero.)*
- ***Item 7d. Data Centers.*** *Provide the number of data centers in which you store Texas HHS Confidential Information. A Data Center is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. If none, answer "0" (zero).*

Item #8. Number of unduplicated individuals for whom the Applicant/Bidder reasonably expects to handle Texas HHS Confidential Information during one year*. Select the radio button that corresponds with the number of clients/consumers for whom you expect to handle Confidential Information during a year. Only count clients/consumers once, no matter how many direct services the client receives during a year.*

Item #9. HIPAA Business Associate Agreement*.*

- ***Item #9a.*** *Answer "Yes" if your business will use, disclose, create, receive, transmit, or store information relating to a client/consumer's healthcare on behalf of the Department of State Health Services, the Department of Disability and Aging Services, or the Health and Human Services Commission for treatment, payment, or operation of Medicaid or Medicaid clients. If your contract does not include HIPAA covered information, respond "no." If "no," a compliance plan is not required.*
- ***Item #9b.*** *Answer "Yes" if your business has a notice of privacy practices (a document that explains how you protect and use a client/consumer's healthcare information) displayed either on a website (if one exists for your business) or in your place of business (if that location is open to clients/consumers or the public). If your contract does not include HIPAA covered information, respond "N/A."*

Item #10. Subcontractors*. If your business responded "0" to question 4 (number of subcontractors), Answer "N/A" to Items 10a and 10b to indicate not applicable.*

- ***Item #10a.*** *Answer "Yes" if your business requires that all subcontractors sign Attachment 1 of the DUA.*
- ***Item #10b.*** *Answer "Yes" if your business obtains Texas HHS approval before permitting subcontractors to handle Texas HHS Confidential Information on your business's behalf.*

Item #11. Optional Insurance. *Answer "yes" if applicant has optional insurance in place to provide coverage for a Breach or any*

other situations listed in this question. If you are not required to have this optional coverage, answer "N/A" A compliance plan is not required.

SECTION B. PRIVACY RISK ANALYSIS AND ASSESSMENT

Reasonable and appropriate written Privacy and Security policies and procedures are required, even for sole proprietors who are the only employee, to demonstrate how your business will safeguard Texas HHS Confidential Information and respond in the event of a Breach of Texas HHS Confidential Information. To ensure that your business is prepared, all of the items below must be addressed in your written Privacy and Security policies and procedures.

Item #1. Answer "Yes" if you have written policies in place for each of the areas (a-o).

- **Item #1a.** Answer "yes" if your business has written policies and procedures that identify everyone, including subcontractors, who are authorized to use Texas HHS Confidential Information. The policies and procedures should also identify the reason why these Authorized Users need to access the Texas HHS Confidential Information and this reason must align with the Authorized Purpose described in the Scope of Work or description of services in the Base Contract with the Texas HHS agency.
- **Item #1b.** Answer "Yes" if your business has written policies and procedures that require your employees (including yourself), your volunteers, your trainees, and any other persons whose work you direct, to comply with the requirements of HIPAA, if applicable, and other confidentiality laws as they relate to your handling of Texas HHS Confidential Information. Refer to the laws and rules that apply, including those referenced in the DUA and Scope of Work or description of services in the Base Contract.
- **Item #1c.** Answer "Yes" if your business has written policies and procedures that limit the Texas HHS Confidential Information you disclose to the minimum necessary for your workforce and subcontractors (if applicable) to perform the obligations described in the Scope of Work or service description in the Base Contract. (e.g., if a client/consumer's Social Security Number is not required for a workforce member to perform the obligations described in the Scope of Work or service description in the Base Contract, then the Social Security Number will not be given to them.) If you are the only employee for your business, policies and procedures must not include a request for, or use of, Texas HHS Confidential Information that is not required for performance of the services.
- **Item #1d.** Answer "Yes" if your business has written policies and procedures that explain how your business would respond to an actual or suspected breach of Texas HHS Confidential Information. The written policies and procedures, at a minimum, must include the three items below. If any response to the three items below are no, answer "no."
  - **Item #1di.** Answer "Yes" if your business has written policies and procedures that require your business to immediately notify Texas HHS, the Texas HHS Agency, regulatory authorities, or other required Individuals or Authorities of a Breach as described in Article 4, Section 4 of the DUA.
    Refer to Article 4, Section 4.01:

    Initial Notice of Breach *must be provided in accordance with Texas HHS and DUA requirements with as much information as possible about the Event/Breach and a name and contact who will serve as the single point of contact with HHS both on and off business hours. Time frames related to Initial Notice include:*
    - *within one hour of Discovery of an Event or Breach of Federal Tax Information, Social Security Administration Data, or Medicaid Client Information*
    - *within 24 hours of all other types of Texas HHS Confidential Information* ***48-hour Formal Notice*** *must be provided no later than 48 hours after Discovery for protected health information, sensitive personal information or other non-public information and must include applicable information as referenced in Section 4.01 (C) 2. of the DUA.*
  - **Item #1dii.** Answer "Yes" if your business has written policies and procedures require you to have and follow a written breach response plan as described in Article 4 Section 4.02 of the DUA.
  - **Item #1diii.** Answer "Yes" if your business has written policies and procedures require you to notify Reporting Authorities and Individuals whose Texas HHS Confidential Information has been breached as described in Article 4 Section 4.03 of the DUA.
- **Item #1e.** Answer "Yes" if your business has written policies and procedures requiring annual training of your entire workforce on matters related to confidentiality, privacy, and security, stressing the importance of promptly reporting any Event or Breach, outlines the process that you will use to require attendance and track completion for employees who failed to complete annual training.

- **Item #1f.** Answer "Yes" if your business has written policies and procedures requiring you to allow individuals (clients/consumers) to access their individual record of Texas HHS Confidential Information, and allow them to amend or correct that information, if applicable.
- **Item #1g.** Answer "Yes" if your business has written policies and procedures restricting access to Texas HHS Confidential Information to only persons who have been authorized and trained on how to handle Texas HHS Confidential Information
- **Item #1h.** Answer "Yes" if your business has written policies and procedures requiring sanctioning of any subcontractor, employee, trainee, volunteer, or anyone whose work you direct when they have accessed Texas HHS Confidential Information but are not authorized to do so, and that you have a method of proving that you have sanctioned such an individuals. If you are the only employee, you must demonstrate how you will document the noncompliance, update policies and procedures if needed, and seek additional training or education to prevent future occurrences.
- **Item #1i.** Answer "Yes" if your business has written policies and procedures requiring you to update your policies within 60 days after you have made changes to how you use or disclose Texas HHS Confidential Information.
- **Item #1j.** Answer "Yes" if your business has written policies and procedures requiring you to restrict attempts to take de-identified data and re-identify it or restrict any subcontractor, employee, trainee, volunteer, or anyone whose work you direct, from contacting any individuals for whom you have Texas HHS Confidential Information except to perform obligations under the contract, or with written permission from Texas HHS.
- **Item #1k.** Answer "Yes" if your business has written policies and procedures prohibiting you from using, disclosing, creating, maintaining, storing or transmitting Texas HHS Confidential Information outside of the United States.
- **Item #1l.** Answer "Yes" if your business has written policies and procedures requiring your business to cooperate with HHS agencies or federal regulatory entities for inspections, audits, or investigations related to compliance with the DUA or applicable law.
- **Item #1m.** Answer "Yes" if your business has written policies and procedures requiring your business to use appropriate standards and methods to destroy or dispose of Texas HHS Confidential Information. Policies and procedures should comply with Texas HHS requirements for retention of records and methods of disposal.
- **Item #1n.** Answer "Yes" if your business has written policies and procedures prohibiting the publication of the work you created or performed on behalf of Texas HHS pursuant to the DUA, or other Texas HHS Confidential Information, without express prior written approval of the HHS agency.

Item #2. Answer "Yes" if your business has a current training program that meets the requirements specified in the SPI for you, your employees, your subcontractors, your volunteers, your trainees, and any other persons under you direct supervision.

Item #3. Answer "Yes" if your business has privacy safeguards to protect Texas HHS Confidential Information as described in the SPI.

Item #4. Answer "Yes" if your business maintains current lists of persons in your workforce, including subcontractors (if applicable), who are authorized to access Texas HHS Confidential Information. If you are the only person with access to Texas HHS Confidential Information, please answer "yes."

Item #5. Answer "Yes" if your business and subcontractors (if applicable) monitor for and remove from the list of Authorized Users, members of the workforce who are terminated or are no longer authorized to handle Texas HHS Confidential Information. If you are the only one with access to Texas HHS Confidential Information, please answer "Yes."

SECTION C. SECURITY RISK ANALYSIS AND ASSESSMENT

This section is about your electronic systems. If you DO NOT store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal computer, mobile device, database, server, etc.), select the "No Electronic Systems" box and respond "Yes" for all questions in this section.

Item #1. Answer "Yes" if your business does not "offshore" or use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information outside of the United States. If you are not certain, contact your provider of technology services (application, cloud, data center, network, etc.) and request confirmation that they do not off-shore their data.

Item #2. Answer "Yes" if your business uses a person or company who is knowledgeable in IT security to maintain or oversee the configurations of your business's computing systems and devices. You may be that person, or you may hire someone who can provide that service for you.

Item #3. Answer "Yes" if your business monitors and manages access to Texas HHS Confidential Information (i.e., reviews systems to ensure that access is limited to Authorized Users; has formal processes for granting, validating, and reviews the need for remote access to Authorized Users to Texas HHS Confidential Information, etc.). If you are the only employee, answer "Yes" if you have implemented a process to periodically evaluate the need for accessing Texas HHS Confidential Information to fulfill your Authorized Purposes.

Item #4. Answer "Yes" if your business has implemented a system for changing the password a system initially assigns to the user (also known as the default password), and requires users to change their passwords at least every 90 days, and prohibits the creation of weak passwords for all computer systems that access or store Texas HHS Confidential Information (e.g., a strong password has a minimum of 8 characters with a combination of uppercase, lowercase, special characters, and numbers, where possible). If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

Item #5. Answer "Yes" if your business assigns a unique user name and private password to each of your employees, your subcontractors, your volunteers, your trainees and any other persons under your direct control who will use, disclose, create, receive, transmit or maintain Texas HHS Confidential Information.

Item #6. Answer "Yes" if your business locks the access after a certain number of failed attempts to login and after 15 minutes of user inactivity on all computing devices that access or store Texas HHS Confidential Information. If your business uses a Microsoft Windows system, refer to the Microsoft website on how to do this, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy

Item #7. Answer "Yes" if your business secures, manages, and encrypts remote access, such as: using Virtual Private Network (VPN) software on your home computer to access Texas HHS Confidential Information that resides on a computer system at a business location or, if you use wireless, ensuring that the wireless is secured using a password code. If you do not access systems remotely or over wireless, answer "Yes."

Item #8. Answer "Yes" if your business updates the computer security settings for all your computers and electronic systems that access or store Texas HHS Confidential Information to prevent hacking or breaches (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit opportunities for hackers or intruders to access your system). For example, Microsoft's Windows security checklist:
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings

Item #9. Answer "Yes" if your business secures physical access to computer, paper, or other systems containing Texas HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.). If you are the only employee and use these practices for your business, answer "Yes."

Item #10. Answer "Yes" if your business uses encryption products to protect Texas HHS Confidential Information that is transmitted over a public network (e.g., the Internet, WIFI, etc.) or that is stored on a computer system that is physically or electronically accessible to the public (FIPS 140-2 validated encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.) For more information regarding FIPS 140-2 encryption products, please refer to: *http://csrc.nist.gov/publications/fips*).

Item #11. Answer "Yes" if your business stores Texas HHS Confidential Information on encrypted end-user electronic devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.) and can produce evidence of the encryption, such as, a screen shot or a system report (FIPS 140-2 encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data). For more information regarding FIPS 140-2 validated encryption products, please refer to: *http://csrc.nist.gov/publications/fips*). If you do not utilize end-user electronic devices for storing Texas HHS Confidential Information, answer "Yes."

Item #12. Answer "Yes" if your business requires employees, volunteers, trainees and other workforce members to sign a document that clearly outlines their responsibilities for protecting Texas HHS Confidential Information and associated systems containing Texas HHS Confidential Information before they can obtain access. If you are the only employee answer "Yes" if you have signed or are willing to sign the DUA, acknowledging your adherence to requirements and responsibilities.

Item #13. Answer "Yes" if your business is willing to perform a criminal background check on employees, subcontractors, volunteers, or trainees who access Texas HHS Confidential Information. If you are the only employee, answer "Yes" if you are willing to submit to a background check.

Item #14. Answer "Yes" if your business prohibits the access, creation, disclosure, reception, transmission, maintenance, and storage of Texas HHS Confidential Information on Cloud Services or social media sites if you use such services or sites, and there is a Texas HHS approved subcontractor agreement that includes compliance and liability clauses with the same requirements as the Applicant/Bidder. If you do not utilize Cloud Services or media sites for storing Texas HHS Confidential Information, answer "Yes."

Item #15. Answer "Yes" if your business keeps current on security updates/patches (including firmware, software and applications) for computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:
https://portal.msrc.microsoft.com/en-us/

Item #16. Answer "Yes" if your business's computing systems that use, disclose, access, create, transmit, maintain or store Texas HHS Confidential Information contain up-to-date anti-malware and antivirus protection. If you use a Microsoft Windows system, refer to the Microsoft website on how to ensure your system is automatically updating, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/

Item #17. Answer "Yes" if your business reviews system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis. If you use a Microsoft Windows system, refer to the Microsoft website for ensuring your system is logging security events, see example:
https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies

Item #18. Answer "Yes" if your business disposal processes for Texas HHS Confidential Information ensures that Texas HHS Confidential Information is destroyed so that it is unreadable or undecipherable. Simply deleting data or formatting the hard drive is not enough; ensure you use products that perform a secure disk wipe. Please see NIST SP 800-88 R1, *Guidelines for Media Sanitization* and the applicable laws and regulations for the information type for further guidance.

Item #19. Answer "Yes" if your business ensures that all public facing websites and mobile applications containing HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.516

SECTION D. SIGNATURE AND SUBMISSION

Click on the signature area to digitally sign the document. Email the form as an attachment to the appropriate Texas HHS Contract Manager.

Exhibit E: Lobbying Certification

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions. Submission of this statement is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

* APPLICANT'S ORGANIZATION

* PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE

Prefix: * First Name: Middle Name:

* Last Name: Suffix:

* Title:

* SIGNATURE: * DATE:

Exhibit E1: Federal Assurances – Non Construction

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

OMB Number: 4040-0007
Expiration Date: 02/28/2022

ASSURANCES - NON-CONSTRUCTION PROGRAMS

Public reporting burden for this collection of information is estimated to average 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0040), Washington, DC 20503.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the awarding agency. Further, certain Federal awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.

2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.

3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.

5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).

6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C.§§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee- 3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.

7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.

8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327-333), regarding labor standards for federally-assisted construction subagreements.

10. Will comply, if applicable, with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is $10,000 or more.

11. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).

12. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

13. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq.).

14. Will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported by this award of assistance.

15. Will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported by this award of assistance.

16. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

17. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."

18. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.

19. Will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from (1) Engaging in severe forms of trafficking in persons during the period of time that the award is in effect (2) Procuring a commercial sex act during the period of time that the award is in effect or (3) Using forced labor in the performance of the award or subawards under the award.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL	TITLE
APPLICANT ORGANIZATION	DATE SUBMITTED

Exhibit F: Fiscal Federal Funding Accountability and Transparency Act (FFATA) Certification

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

EXHIBIT F to HHSC Agreement TBD

Fiscal Federal Funding Accountability and Transparency Act (FFATA) CERTIFICATION

The certifications enumerated below represent material facts upon which HHSC relies when reporting information to the federal government required under federal law. If the Department later determines that the Contractor knowingly rendered an erroneous certification, HHSC may pursue all available remedies in accordance with Texas and U.S. law. Signor further agrees that it will provide immediate written notice to HHSC if at any time Signor learns that any of the certifications provided for below were erroneous when submitted or have since become erroneous by reason of changed circumstances. ***If the Signor cannot certify all of the statements contained in this section, Signor must provide written notice to HHSC detailing which of the below statements it cannot certify and why*.**

Legal Name of Contractor:	**FFATA Contact # 1 Name, Email and Phone Number:**
Primary Address of Contractor:	**FFATA Contact #2 Name, Email and Phone Number:**
ZIP Code: 9-digits Required www.usps.com ☐☐☐☐☐ - ☐☐☐☐	**DUNS Number: 9-digits Required www.sam.gov** ☐☐☐☐☐☐☐☐☐
State of Texas Comptroller Vendor Identification Number (VIN) 14 Digits ☐☐☐☐☐☐☐☐☐☐☐☐☐☐	

Printed Name of Authorized Representative	**Signature of Authorized Representative**
Title of Authorized Representative	**Date**

Fiscal Federal Funding Accountability and Transparency Act (FFATA) CERTIFICATION

As the duly authorized representative (Signor) of the Contractor, I hereby certify that the statements made by me in this certification form are true, complete and correct to the best of my knowledge.

Did your organization have a gross income, from all sources, of less than $300,000 in your previous tax year? ☐ Yes ☐ No

If your answer is "Yes", skip questions "A", "B", and "C" and finish the certification.
If your answer is "No", answer questions "A" and "B".

A. Certification Regarding % of Annual Gross from Federal Awards.

Did your organization receive 80% or more of its annual gross revenue from federal awards during the preceding fiscal year? ☐ Yes ☐ No

B. Certification Regarding Amount of Annual Gross from Federal Awards.

Did your organization receive $25 million or more in annual gross revenues from federal awards in the preceding fiscal year? ☐ Yes ☐ No

If your answer is "Yes" to both question "A" and "B", you must answer question "C".
If your answer is "No" to either question "A" or "B", skip question "C" and finish the certification.

C. Certification Regarding Public Access to Compensation Information.

Does the public have access to information about the compensation of the senior executives in your business or organization (including parent organization, all branches, and all affiliates worldwide) through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986? ☐ Yes ☐ No

If your answer is "Yes" to this question, where can this information be accessed?

If your answer is "No" to this question, you must provide the names and total compensation of the top five highly compensated officers below.

For example:

John Blum:500000;Mary Redd:50000;Eric Gant:400000;Todd Platt:300000; Sally Tom:300000

Provide compensation information here:

Fiscal Federal Funding Accountability and Transparency Act (FFATA) CERTIFICATION

Exhibit G: Assumptions and Exceptions Form

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

Exhibit G
Assumptions and Exceptions Form

(NOTE TO Vendors: COMPLETION OF THIS EXHIBIT IS NOT REQUIRED IF THERE ARE NO ASSUMPTIONS. SEE SOW SECTION 3.6.6)
No assumption -- nor any term, condition, or provision in a Solicitation Response that differs, varies from, or contradicts this Solicitation -- will be considered to be a part of any contract resulting from this Solicitation unless expressly made a part of the contract in writing by the HHSC.

List Assumptions here.

Solicitation Document	Solicitation Document Section Number	Solicitation Language for which Assumption is Made (set forth language from solicitation)	Basis of Assumption	Vendor's Language for Assumption	Does Vendor want to be considered for Contract Award if Assumption is denied? (State "Yes" or "No")

Exhibit G
Assumptions and Exceptions Form

(NOTE TO Vendors: COMPLETION OF THIS EXHIBIT IS NOT REQUIRED IF THERE ARE NO EXCEPTIONS. SEE SOW SECTION 3.6.5)
No exception -- nor any term, condition, or provision in a Solicitation Response that differs, varies from, or contradicts this Solicitation -- will be considered to be a part of any contract resulting from this Solicitation unless expressly made a part of the contract in writing by the HHSC.

List Exceptions here

Solicitation Document	Solicitation Document Section Number	Solicitation Language for which Exception is Made (set forth language from solicitation)	Basis of Exception	Vendor's Proposed Language for Exception	Still Want to be Considered for Contract Award if Exception Is Denied? (State "Yes" or "No")

Exhibit H: Proposal Evaluation Tool

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

TIERS Cloud Assessment and Migration Planning Services
Criteria, Subcriteria Sheet
SOW No. HHS0006347

Evaluator				
Respondent				
#	Criteria	Weight	Score	Comments - Required for all scores
1	EVALUATION CRITERIA 1 - Project Approach			
1.1	Article V Narrative Proposal - Section 5.1 - Executive Summary Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 5.1	5.0%		
1.2	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 1 - TIERS Inventory Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.1	2.0%		
1.3	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 2 - TIERS Cloud Assessment Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.2	2.0%		
1.4	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 3 - Application Transformation Planning Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.3	2.0%		
1.5	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 4 - Cloud Security Planning Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.4	2.0%		
1.6	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 5- Cloud Migration Planning Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.5	2.0%		
1.7	Article V Narrative Proposal - Section 5.2 - Project Approach - Phase 6 - Post-Migration Planning Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.3.6	2.0%		
1.8	Article V Narrative Proposal - Section 5.4 - Project Work Plan Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 2.1.4	5.0%		
1.9	Article V Narrative Proposal - Section 5.5 - Example Work Products Evaluate and score Vendor Response, by reviewing how best the vendor proposal meets the objectives and criteria of the SOW requirements in Section 5.5	5.0%		
1.10	Narrative Proposal - Exhibit G - Assumptions and Exceptions Form HHSC will more favorably evaluate responses that offer no or few exceptions, reservations, or limitations to the terms and conditions of the solicitation (ref Section 3.5.5).	3.0%		
	Subtotal	**30.0%**		
2	EVALUATION CRITERIA 2 - Personnel Organization and Qualifications			
2.1	Article V Narrative Proposal - Section 5.3 - Staffing Plan Review Vendor's Staffing Plan to meet the requirements in Article II Scope of Work in the SOW.	10.0%		
2.2	Article V Narrative Proposal - Section 5.3 - Staffing Plan - Staff Resumes Review resource expertise and experience to meet the requirements in Article II Scope of Work in the SOW.	10.0%		
	Subtotal	**20.0%**		
3	EVALUATION CRITERIA 3 - Vendor Capabilities and Performance			
3.1	Article VI Required Respondent Information - Section 6.1 - Company Information Evaluate and score Vendor Response to review the Company Narrative and Company Profile to assess the Vendors key strengths and competitive advantages for fulfilling the requirements in Article II Scope of Work in this SOW	10.0%		
3.2	Article VI Required Respondent Information - Section 6.2 - Past Performance Evaluate and score Vendor Response for vendor and/or its subcontractor(s) experience as described in Section 6.2. Evaluate the Vendor strengths to meet the requirements of Article II Scope of Work in this SOW.	6.0%		
3.3	Article VI Required Respondent Information - Section 6.3 - Major Sub Contractor Information Evaluate and score Vendor Response Major Sub Contractor information to review the Company Narrative and Company Profile to assess the Vendors key strengths and competitive advantages for fulfilling the requirements in Article II Scope of Work in this SOW	2.0%		
3.4	Article VI Required Respondent Information - Section 6.4 - Litigation and Contract History & Section 6.5 - Conflicts Evaluate and score Vendor Response for any potential risks to HHSC.	2.0%		
	Subtotal	**20.0%**		
4	EVALUATION CRITERIA 4 - Cost			
4.1	Article VII Cost Proposal - Section 7.1 - Attachment E Service Rate Schedule Evaluate and score Vendor Response is substantially aligned with the SOW requirements.	10.0%		
4.2	Article VII Cost Proposal - Section 7.1 - Attachment F Deliverable Cost Schedule Evaluate and score Vendor Response is substantially aligned with the SOW requirements.	15.0%		
4.3	Article VII Cost Proposal - Exhibit G, Assumptions and Exceptions HHSC will more favorably evaluate responses that offer no or few exceptions, reservations, or limitations to the terms and conditions of the solicitation (ref Section 3.5.5).	5.0%		
	Subtotal	**30.0%**		
	TOTAL (%)	**100.0%**		

Exhibit I:
Services Rate Schedule

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

EXHIBIT I: SERVICES RATE SCHEDULE

INSTRUCTIONS:

The Respondent must complete the rate table below for all resources and roles included in the response. In addition, the Respondent shall commit to using the Hourly Rates for all change orders. Any additional services shall be quoted as firm fixed price Deliverables inclusive of all Vendor costs. Pricing for such Deliverables shall be based upon the Hourly Rates in this exhibit.

Named Resource Or FTE[1]	Project Role[2]	DIR Category/Title/Level[3]	Hourly Rate[4]
	Project Manager		

Note: Additional rows can be inserted as needed.

1 – List all named resources from the Staffing Plan in the response (one per line).

2 – Identify the project role for each resource.

3 – Identify a Category, Title, and Level for each resource that conforms to the Texas Department of Information Resources (DIR) IT Services Contract (ITSAC) Not-to-Exceed rate document. The document can be found at http://dir.texas.gov/ using the search feature for "ITSAC Not to Exceed Rates".

4 – All Vendor costs must be included in the rates, except for hardware, software, tools, supplies and other support to be provided by HHSC as described in SOW Section 2.1.7.

Exhibit J:
Deliverable Cost Schedule

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission
(HHSC)

EXHIBIT J: DELIVERABLE COST SCHEDULE

INSTRUCTIONS:

Please enter the Respondent's fixed price for each Deliverable in table 1 below and optional Phase 7 Migration Support Services fixed price for each payment item in table 2 below. All Vendor costs must be included in the price, except for hardware, software, tools, supplies and other support to be provided by HHSC as described in SOW Section 2.1.7.

Table 1 – Base Contract Deliverables

Deliverable ID	Deliverable Description	Price
1	Project Work Plan	
2	Phase 1 – TIERS Inventory	
3	Phase 2 – TIERS Cloud Assessment	
4	Phase 3 – Application Transformation Plan	
5	Phase 4 – Cloud Security Plan	
6	Phase 5 – Cloud Migration Plan	
7	Phase 6 – Post-Migration Plan	
	CONTRACT TOTAL COST	

Table 2 – Phase 7 – Migration Support Services (Optional)

Payment Item #	Contract Artifact ID	Price
1	Migration Support Services – Month 1	
2	Migration Support Services – Month 2	
3	Migration Support Services – Month 3	
4	Migration Support Services – Month 4	
5	Migration Support Services – Month 5	
6	Migration Support Services – Month 6	
	PHASE 7 TOTAL COST	

Note: If HHSC elects to request Migration Support Services for more than six (6) months, the cost for the additional support months will be based on the per item price in table 2.

Exhibit K:
Past Performance Template

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Exhibit K
Past Performance Template

General Instructions

For each matter listed, the Respondent must complete a past performance template.

Respondent shall list and provide information concerning a minimum of three (3) contracts or projects similar to the services enumerated in Article II. HHSC prefers projects or contracts that were performed for states of comparable size and/or federal government within the last five (5) years. Respondents must verify client contacts are current. If you list HHSC contracts or projects leave blank information regarding client contact. The Vendor must provide the following information for each project reference as outlined in the **past performance template** on pages 3-4 of this document:

1. Project Name
2. Name and address of client
3. Name and phone number of client contact (contract or project manager)
4. Email address for client contact
5. Contract start date and duration
6. Total Cost of contract/project
7. Contract/Project Description
8. Staff assigned to the referenced contract/project designated for work under this Solicitation
9. Outcome of the project

Past Performance Template (To Be Completed By Respondent)

Project Name:	
Name and Address of client:	
Name and phone number of client contact:	
Email address of client contact:	
Contract start date and duration:	
Total Contract Dollar Amount:	
Brief description of project:	

Staff assigned by position on the project:
Outcome of the project:

Exhibit L: Vendor Information and Disclosures

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Exhibit L
Vendor Information and Disclosures

Instructions: This form must be submitted as an attachment to the Vendor's proposal.

Part 1: General Vendor Information.

1. Organization's Legal Name and number of employees: _____
2. Doing Business As: _____
3. Physical Address: _____
4. Mailing Address: _____
5. Taxpayer Identification Number: _____
6. Legal Status (check one): ☐ For-profit Entity ☐ Non-profit Entity ☐ Governmental Entity
7. Business Structure (check one): ☐ Corporation ☐ Limited (Liability) Company ☐ Partnership ☐ Limited (Liability) Partnership ☐ Joint Venture ☐ Sole Proprietorship ☐ Other (specify): _____
8. Date and State of Incorporation, If Applicable: _____
9. Name of Parent Entity and percentage ownership, If Applicable: _____
10. HUB Status (check one): ☐ State of Texas Certified Entity ☐ Non-HUB Entity

Part 2: Vendor Contact Information.

1. Person Who Will Sign the Contract:	2. Primary Contact for Proposal Questions:
Name: _____	Name: _____
Title: _____	Title: _____
Mailing Address: _____	Mailing Address: _____
Telephone: _____	Telephone: _____
Fax: _____	Fax: _____
E-mail: _____	E-mail: _____

Part 3: Subcontractor Information. ***Provide the following information for each proposed subcontractor. Attach additional pages if necessary.***

1. Organization's Legal Name and number of employees: _____
2. Doing Business As: _____
3. Physical Address: _____

4. Mailing Address: _____
5. Taxpayer Identification Number: _____
6. Legal Status (check one): ☐ For-profit Entity ☐ Non-profit Entity ☐ Governmental Entity
7. Business Structure (check one): ☐ Corporation ☐ Limited (Liability) Company ☐ Partnership ☐ Limited (Liability) Partnership ☐ Joint Venture ☐ Sole Proprietorship ☐ Other (specify): _____
8. Date and State of Incorporation, If Applicable: _____
9. Name of Parent Entity, and percentage ownership, If Applicable: _____
10. HUB Status (check one): ☐ State of Texas Certified Entity ☐ Non-HUB Entity

Have you attached additional pages for Part 3? ☐ Yes ☐ No

Part 4: Former Employees of a State Agency. ***Identify all Vendor or subcontractor personnel who have worked for HHSC or another health and human services agency in the past two years. Attach additional pages if necessary.***

1. Name of former state employee: _____
2. Job title at termination of state employment: _____
3. Date of termination of state employment: _____
4. Annual rate of compensation at termination: _____
5. Description of job responsibilities while state employee: _____

_____

_____

_____

_____

6. If the former state employee worked on matters relating to the RFP, describe those matters:

_____

_____

_____

_____

_____

Have you attached additional pages for Part 4? ☐ Yes ☐ No

Part 5: Conflicts of Interest. ***Describe all facts or circumstances that may give rise to a potential conflict of interest, and describe all measures the Vendor and its subcontractors will take to ensure that these facts or circumstances do not create an actual conflict of interest. Attach additional pages if necessary.***

Have you attached additional pages for Part 5? ☐ Yes ☐ No

Part 6: Litigation. ***Disclose all pending, resolved, or completed litigation, mediation, arbitration, or other alternative dispute resolution procedure involving the Vendor within the past 60 months. Include the cause number, court, parties' names, subject matter, relief sought, amount in controversy, and final disposition or status. Provide the same information for all subcontractors. Attach additional pages if necessary.***

Have you attached additional pages for Part 6? ☐ Yes ☐ No

Part 7: Texas Public Information Act (PIA): ***Complete this part if you assert one or more parts of the proposal are excepted from disclosure under the PIA. Attach additional pages if necessary.***
1. Proposal Section: _____ 2. PIA Exception*: _____ 3. Explanation of Why the Exception Applies: _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

* The most commonly asserted exception is Texas Government Code §552.110 (trade secret, or commercial or financial information confidential by law).

Have you attached additional pages for Part7? Yes ☐ No ☐

Exhibit M:
Vendor Insurance Coverage

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Exhibit M
Vendor Insurance Coverage

Contractor shall maintain at its own cost and expense, in full force and effect during performance of the Services, the following insurance coverages and limits:

1. **Workers' Compensation.**
    a. Insurance with limits as required by the Texas Workers' Compensation Act, with the policy endorsed to provide a waiver of subrogation in favor of HHSC, and employer's liability insurance of not less than:
        i. $1,000,000 each accident;
        ii. $1,000,000 disease each employee; and
        iii. $1,000,000 disease policy limit.
    b. Workers' compensation insurance coverage must be provided for all workers at all tier levels and meet the statutory requirements of Tex. Lab. Code §401.011(44).

2. **Commercial General Liability Insurance.**
    a. Including premises, operations, independent Vendor 's liability, products and completed operations and contractual liability, covering, but not limited to, the liability assumed under the indemnification provisions of this Contract, fully insuring Vendor 's liability for bodily injury (including death) and property damage with a minimum limit of:
        i. $1,000,000 per occurrence;
        ii. $2,000,000 general aggregate;
        iii. $5,000 Medical Expense each person;
        iv. $1,000,000 Personal Injury and Advertising Liability;
        v. $2,000,000 products and completed operations aggregate;
        vi. $50,000 Damage to Premises Rented to You; and
        vii. Coverage shall be on an "occurrence" basis

3. **Comprehensive Automobile Liability Insurance**
    a. Covering owned, hired, and non-owned vehicles, with a minimum combined single limit for bodily injury (including death) and property damage of $1,000,000 per accident. No aggregate shall be permitted for this type of coverage.

4. **Umbrella Liability Insurance**
    a. Vendor shall obtain, pay for and maintain umbrella liability insurance during the Contract term, insuring Vendor for an amount of not less than amount of $1,000,000 Each Claim / $1,000,000 Aggregate and that provides coverage at least as broad as and applies in excess and follows form of the primary liability coverages required hereinabove. The policy shall provide "drop down" coverage where underlying primary insurance coverage limits are insufficient or exhausted.

5. **Cyber/Privacy Liability Insurance Policy**
    a. Vendor shall provide Cyber/Privacy Liability Insurance to cover risk of loss to electronic data. The policy must include coverage in the minimum amount specified below for electronic vandalism to electronic data, including coverage for a third party's willful electronic alteration of data, introduction of viruses which impact electronic data, unauthorized use of electronic data, or denial of service to web site or email destinations.
        i. Cyber Liability Insurance $1,000,000 Claim/$1,000,000 Aggregate.

6. **Professional Liability Insurance**
    a. Vendor shall obtain, pay for and maintain professional liability errors and omissions insurance during the Contract term, insuring Vendor for an amount of not less than $1,000,000 Each Claim / $1,000,000 Aggregate.

General Insurance Requirements:

1. Vendor shall carry insurance in the types and amounts indicated in this Exhibit for the duration of the Contract. The insurance shall be evidenced by delivery to HHSC of certificates of insurance executed by the insurer or its authorized agent stating coverages, limits, expiration dates and compliance with all applicable required provisions. Upon request, HHSC, and/or its agents, shall be entitled to receive without expense, copies of the policies and all endorsements.

2. Vendor shall update all expired policies prior to submission for monthly payment.

3. Failure to update policies shall be reason for withholding of payment until renewal is provided to HHSC.

4. Vendor shall provide and maintain all insurance coverage with the minimum amounts described above until the end of the contract period unless otherwise stated.

5. Failure to maintain insurance coverage, as required, is a material breach of contract and grounds for suspension of Work or termination of the Contract.

6. Vendor shall deliver to HHSC true and complete copies of certificates and corresponding policy endorsements within five (5) business days of Contract execution.

7. Failure of HHSC to demand such certificates or other evidence of Vendor 's full compliance with these insurance requirements or failure of HHSC to identify a deficiency in compliance from the evidence provided shall not be construed as a waiver of Vendor 's obligation to maintain such insurance.

8. The insurance and insurance limits required herein shall not be deemed as a limitation on Vendor 's liability under the indemnities granted to HHSC in the Contract Documents.

9. The insurance coverage and limits established herein shall not be interpreted as any representation or warranty that the insurance coverage and limits necessarily will be adequate to protect Vendor.

10. Coverage shall be written on an occurrence basis by companies authorized and admitted to do business in the State of Texas and rated A or better by A.M. Best Company or similar rating company or otherwise acceptable to HHSC.

Policies must include the following clauses, as applicable:

1. This insurance shall not be canceled, materially changed, or nonrenewed except after thirty (30) days written notice has been given to HHSC.

2. It is agreed that Vendor 's insurance shall be deemed primary with respect to any insurance or self-insurance carried by HHSC for liability arising out of operations under the Contract with HHSC.

3. HHSC, its officials, directors, employees, representatives, and volunteers are added as additional insureds as respects operations and activities of, or on behalf of the named insured performed under Contract with HHSC. The additional insured status must cover completed operations as well. This is not applicable to workers' compensation policies.

4. A waiver of subrogation in favor of HHSC shall be provided in all policies.

5. Without limiting any of the other obligations or liabilities of Vendor, Vendor shall require each Subcontractor performing work under the Contract, at Subcontractor's own expense, to maintain during the term of the Contract, the same stipulated minimum insurance including the required provisions and additional policy conditions as shown above. As an alternative, Vendor may include its Subcontractors as additional insureds on its own coverage as prescribed under these requirements. Vendor's certificate of insurance shall note in such event that Subcontractors are included as additional insureds and that Vendor agrees to provide workers' compensation for Subcontractors and their employees. Vendor shall obtain and monitor the certificates of insurance from each Subcontractor in order to assure compliance with the insurance requirements. Vendor must retain the certificates of insurance for the duration of the Contract plus five (5) years and shall have the responsibility of enforcing these insurance requirements among its Subcontractors. HHSC shall be entitled, upon request and without expense, to receive copies of these certificates.

Attachment A: HHSC and TIERS Background Information

Texas Integrated Eligibility Redesign System (TIERS)

Cloud Assessment and Migration Planning Services

Health and Human Services Commission (HHSC)

Statement of Work (SOW)

Table of Contents

1 HHS INFORMATION 3

1.1 HHS Vision 3

1.2 HHS Mission 3

1.3 HHS agencies and Departments 3

1.3.1 Texas Health and Human Services Commission 4

1.3.2 Texas Department of State Health Services (DSHS) 4

2 HHS IT ORGANIZATION 5

3 TIERS BACKGROUND 7

4 ACRONYMS AND ABBREVIATIONS 10

1 HHS INFORMATION

1.1 HHS VISION

Making a difference in the lives of the people we serve.

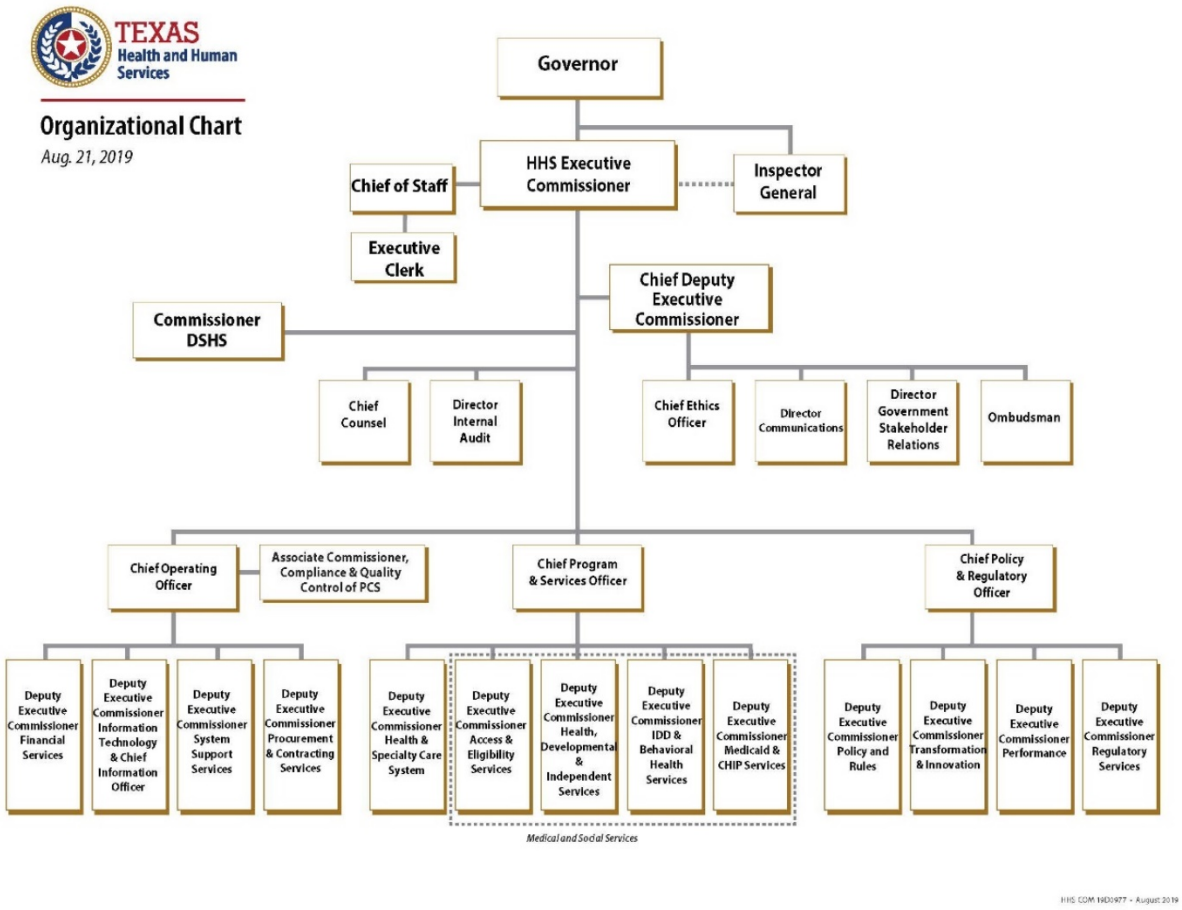
1.2 HHS MISSION

Improving the health, safety and well-being of Texans with good stewardship of public resources.

1.3 HHS AGENCIES AND DEPARTMENTS

Texas Health and Human Services (HHS) consists of two agencies: Texas Health and Human Services Commission and Texas Department of State Health Services.

Information regarding HHSC and its programs is available online and can be accessed at: https://hhs.texas.gov/. The high-level HHS organizational structure is depicted below.



1.3.1 Texas Health and Human Services Commission Summary

Experienced HHSC employees deliver benefits and services, including:

- Medicaid for families and children.
- Long-term care for people who are older or who have disabilities.
- Supplemental Nutrition Assistance Program food benefits and Temporary Assistance for Needy Families cash assistance.
- Behavioral health services.
- Services to help keep people who are older or who have disabilities in their homes and communities.
- Services for women and people with special health needs.

The agency also oversees regulatory functions including:

- Licensing and credentialing long-term care facilities, such as nursing homes and assisted living.
- Licensing child care providers.
- Managing the day-to-day operations of state supported living centers and state hospitals.

1.3.2 Texas Department of State Health Services (DSHS) Summary

Many direct client services performed by DSHS, such as services for women, children and people with special health care needs transferred to HHSC in September 2016. The agency's mission is to improve the health, safety and well-being of Texans through good stewardship of public resources and a focus on core public health functions.

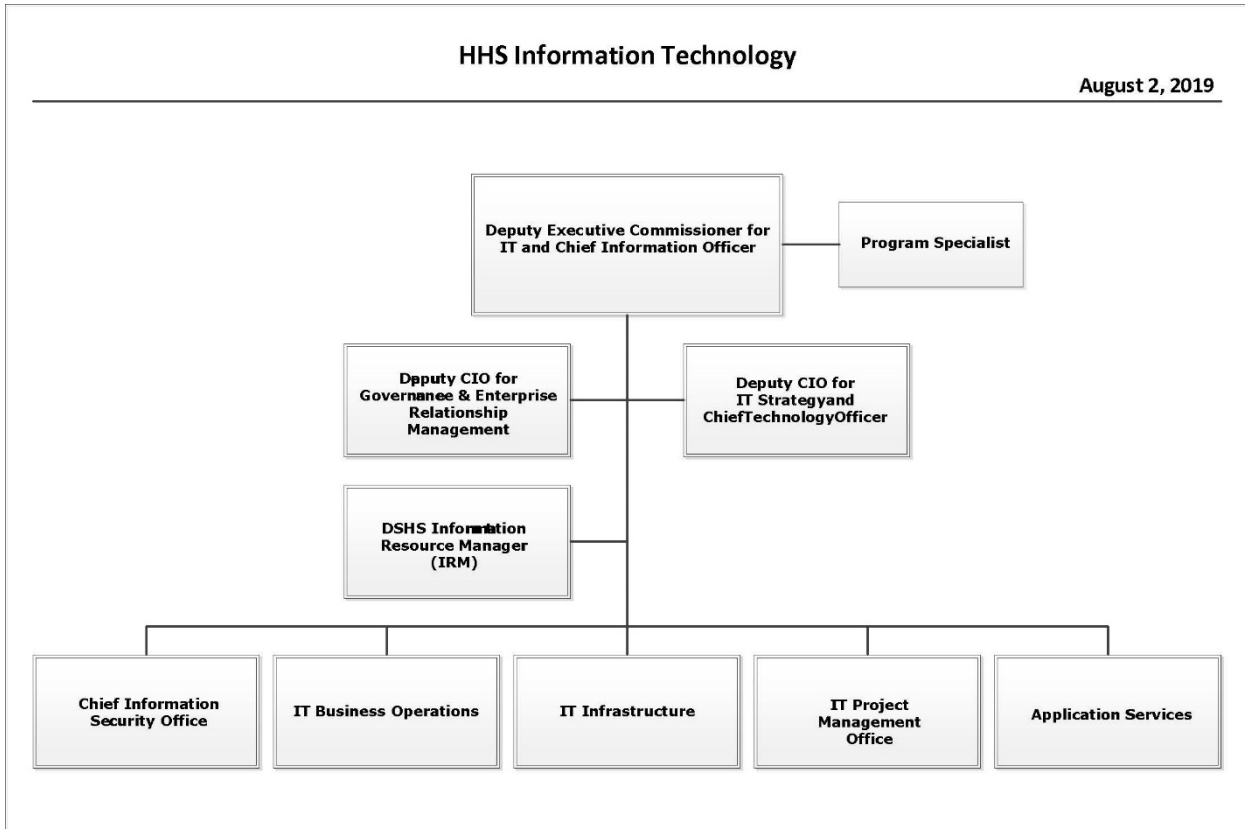
DSHS is well-positioned to provide statewide leadership to promote safe and healthy communities and population-based strategies to address public health issues.

DSHS serves as the population and public health authority for Texas by:

- Providing vital statistics, such as birth and death records.
- Compiling and disseminating health data on numerous topics.
- Administering chronic and infectious disease prevention and laboratory testing efforts.
- Leading the public health response to disasters, disease threats and outbreaks.
- Licensing and regulating facilities on topics from asbestos to mobile food establishments to youth camps.

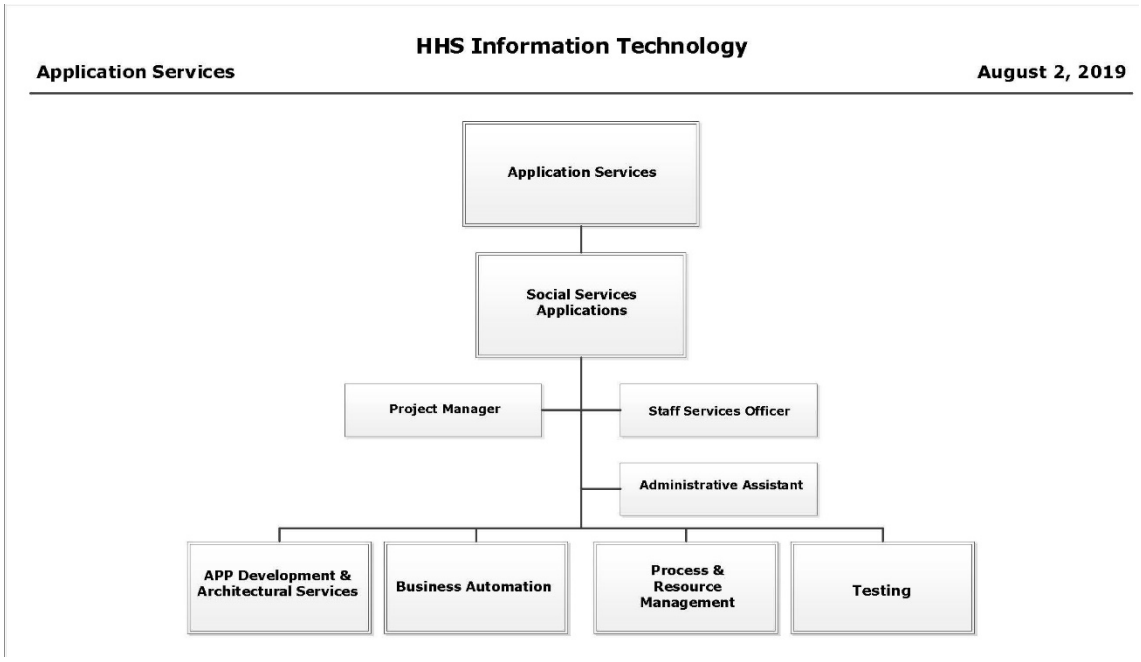
2 HHS IT ORGANIZATION

The HHS Information Technology (IT) division consists of six organizational units as depicted below:

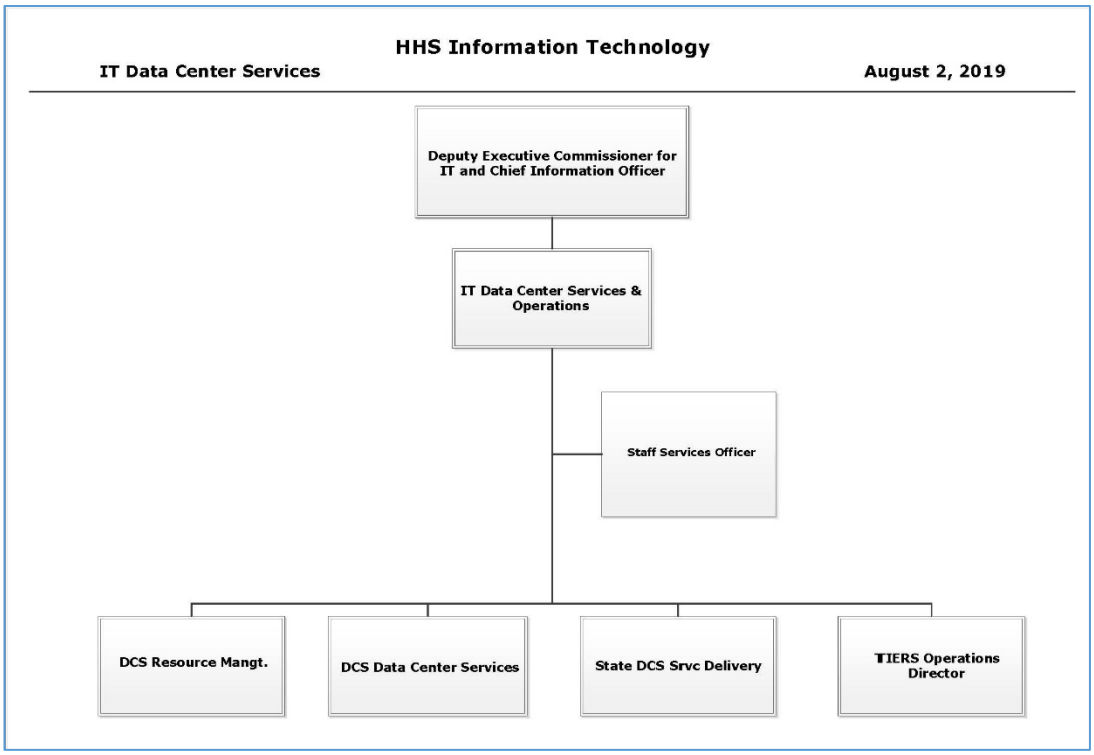


Three of these units are responsible for the major components of TIERS: Application Services, Data Center Services and Operations, and IT Infrastructure. The remaining units play vital roles in support of TIERS.

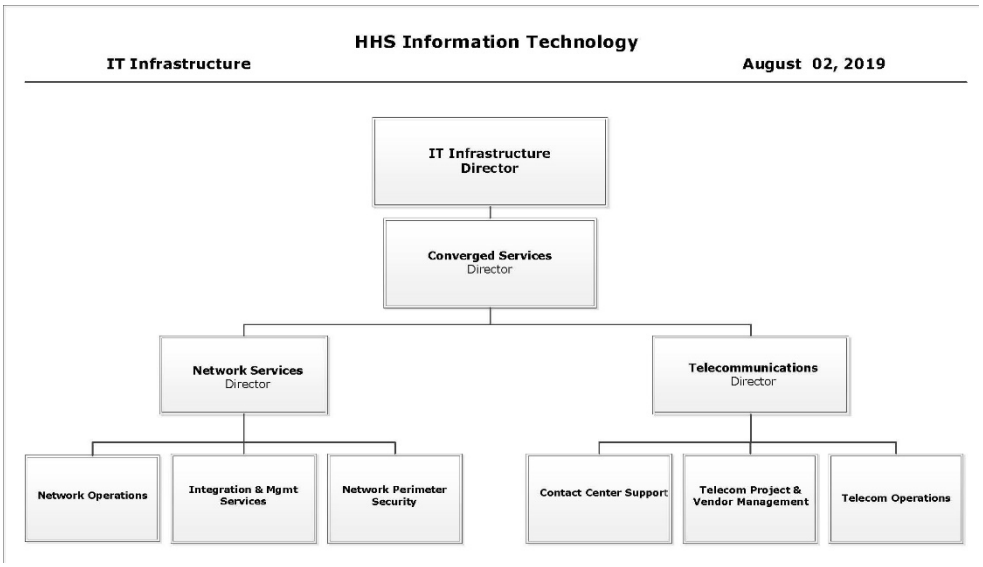
The Social Services Applications department within Application Services is responsible for all the TIERS Applications:



The TIERS Operations department within Data Center Services and Operations is responsible for the TIERS data centers:



The TIERS network operations are supported with Data Center Services and Operations is responsible for the TIERS data centers IT Infrastructure.



3 TIERS BACKGROUND

TIERS is the integrated eligibility system managing delivery of sixty-four (64) types of assistance including food, cash, medical, and community care services to Texans in need. Over 10,000 unique users rely on TIERS every day. TIERS automates complex rule-based processing ensuring consistency in eligibility determination. (Refer to the TIERS Functional and Technical Overview document, also located in the Procurement Library, for additional information). The integration of Information Technology reduces the need for repetitive data-entry and document handling tasks. Serving more than eight (8) million recipients annually, TIERS is a mission critical system for HHSC, and for the State of Texas.

The TIERS eligibility process is by design a rigorous process that takes a complete look at a household. Because it is designed to support an integrated approach to eligibility, TIERS collects a large number of data elements. This requires some additional time at initial application but simplifies the process of recertification, saving time overall; strengthens fraud prevention; and provides a higher level of confidence in the state's ability to accurately determine a family's eligibility for state assistance.

- TIERS collects information on the client and then applies policy to determine the programs for which the client may be eligible and uses the same data for all programs to maintain quality control.
- TIERS and its supporting technologies create an electronic record that follows the client. This flexibility also allows casework to be distributed between offices to balance workloads. Changes made in TIERS are

real-time and are instantly accessible to other workers and entities that interface with the system.

- TIERS allows tasks, such as basic data entry and casework, to be separated and assigned to the most appropriate staff.
- TIERS automatically and uniformly applies all program policies including household composition and budget calculations.

The TIERS and EST Applications include multiple user-facing applications, including the main TIERS module. Many other applications fully integrate with the TIERS and EST Applications. In addition, TIERS has over 30 trading partners, and most of those have multiple interfaces. TIERS applications also include 11,000 business rules, over 3,000 user screens, and more than 2,000 database tables. There are two (2) Data Centers supporting the TIERS infrastructure, which includes 28 environments, and over 800 servers.

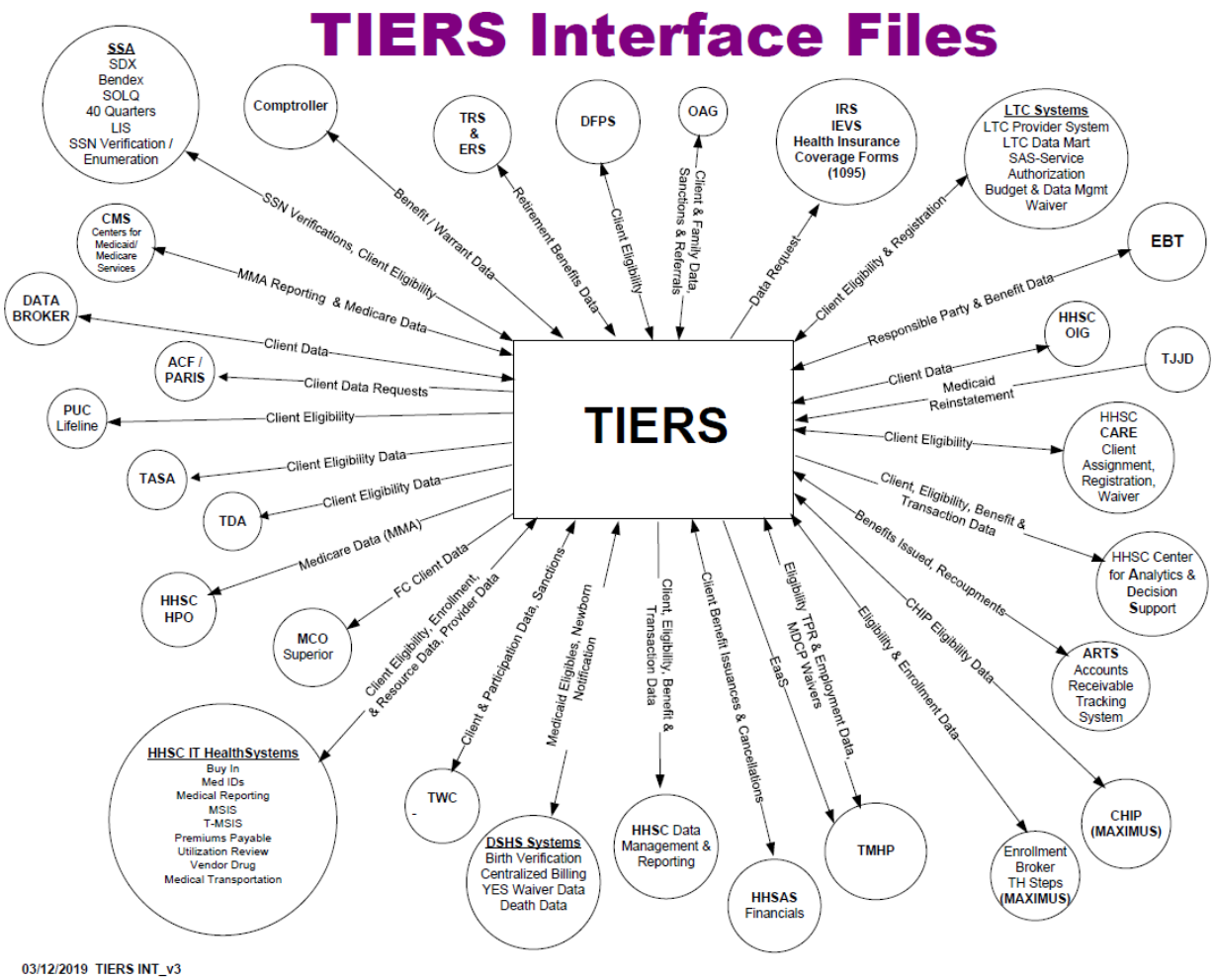
TIERS and EST Applications users include:

- Clients (comprised of individuals or families applying for or receiving government assistance, and those helping clients access benefits)
- Community Based Organizations (CBOs)
- Customer Service Representatives (CSRs)
- HHSC staff and other State of Texas agency staff
- Trading Partners

TIERS processes applications, determines eligibility for HHSC public assistance programs and supports other functions of the Access and Eligibility Services (AES). TIERS internal stakeholders include, but are not limited to, the following HHS areas:

- Access and Eligibility Services (AES)
- Medical and Social Services Division (MSS)
- Medicaid and CHIP Services (MCS)
- Inspector General (IG)

TIERS exchanges data with over thirty (30) Trading Partners most of which have multiple interfaces, as depicted on Page 9.



TIERS is implemented across the State of Texas. The system is required to support users accessing its services in different operational models (e.g., face-to-face interviews, call centers, among others). Table 1 provides a high-level census of the user community.

Table 1 - Major TIERS User Groups and User Volume

Category	User activities	Number of TIERS Users
HHSC Office of Eligibility Services	Eligibility operations (collect data, process cases, etc.). Includes Eligibility Workers and other OES staff that will use TIERS in local eligibility offices, Customer Care Centers, and other centralized Units including ART, MEPD, Data Integrity, and Service Improvement (SIP). ■ Eligibility staff assigned to hearings and appeals. ■ OES staff for CHIP, EB and Complaints	7,775
HHSC Office of Family Services	Case reading and review, quality management, training	358

Category	User activities	Number of TIERS Users
Eligibility Support Vendors — CHIP and Enrollment	Primarily inquiry and file clearance; when CHIP is converted to TIERS: CHIP case processing and eligibility determination	1,167
Eligibility Support Vendors — Customer Care Centers	Eligibility Support: inquiry and data entry. These workers use the State Portal to do certain updates such as address and phone number changes and appointment scheduling which also update TIERS through web services.	3,000
HHSC Office of the Inspector General	Research to clear data matches, determine overpayments, investigate fraud, and impose disqualifications	230
HHSC Hearings and Appeals	Review eligibility information for cases; process hearings and appeals, appointment notices, decisions	110
HHSC Ombudsman	Independent reviews and resolution of complaints	47
HHSC Enterprise Applications	User, technical, development, infrastructure, administrative, and business support; the Central Help Desk, and On-Site Support at benefits offices statewide	580
Non-HHSC agencies	Includes agencies such as DFPS, TWC, etc.; research cases and client data	4,000

4 GLOSSARY, ACRONYMS AND ABBREVIATIONS

Table 2 summarizes the acronyms and abbreviations used by TIERS and is provided for additional clarity.

Table 2 – Glossary, Acronyms and Abbreviations

Acronym / Term	Description
ACA	**Affordable Care Act** The health care reform law enacted in March 2010
ACL	**Access Control List** An access control list is an implementation of logical rules to permit or deny certain packets to go through an interface; generally used in firewalls.
API	**Application Programming Interface** In computer programming, an **application programming interface** (**API**) is a set of routines, protocols, and tools for building software applications.
ARS	**Acceptable Risk Safeguards**

Acronym / Term	Description
	A broad set of the Centers for Medicare and Medicaid Services (CMS) security controls, which are based on NIST requirements.
CBO	**Community Based Organizations** Community based organizations operate at the local level to provide services and assistance to community members in need.
CCI	**Call Center Inquiry** The Call Center Inquiry application assists CCRs in rapidly collecting TIERS information on a specific client or case.
CHIP	**Children's Health Insurance Program**
CISO	**Chief Information Security Officer** A senior-level executive responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets are adequately protected.
CIS	**Center for Internet Security** The Center for Internet Security (CIS) is a not-for-profit organization focused on enhancing the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration.
CMS	**Centers for Medicare & Medicaid Services** Federal agency that administers Medicare, Medicaid, and the Children's Health Insurance Program
CSR	**Customer Service Representative** Vendor employees who provide clients with telephone assistance regarding overviews of eligibility programs and services, answers to application and eligibility questions, receive changes, and assist with screening and application completion.
Data Center	A **Data Center** is a dedicated space within a secure building facility, or a group of building facilities used to house computer systems, containing client data and other associated components such as telecommunications, power supply, special cooling systems, and storage systems. The data center allows computer transactions to be carried out for related business and customer domains.
DDoS	**Distributed Denial of Service** An attempt to make a computer or network resource unavailable to its intended users.
DHCP	**Dynamic Host Configuration Protocol** A network configuration protocol for hosts on Internet Protocol (IP) networks. The most essential communication configuration information is an IP address, and a default route and routing prefix. DHCP automates that task and provides a central database of devices that are connected to the network, eliminating duplicate resource assignments.
DLP	**Data Loss Prevention** Technology used to control and manage data flows in order to prevent leakage of confidential and sensitive information.
DMZ	**Demilitarized Zone**

Acronym / Term	Description
	A DMZ is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.
DR	**Disaster Recovery** Disaster recovery involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
ECM	**Enterprise Content Manager** System to capture, manage, store, preserve, and deliver content and documents related to TIERS processes.
EDS	**Enterprise Document Services** EDS was implemented as a PDF generating engine for producing and merging documents, and primarily provides this service to other applications in the middleware layer.
EISSG	**Enterprise Information Security Standards and Guidelines (Texas)** A State of Texas document that, along with the Enterprise Information Security Policy document, serves to protect Health and Human Services (HHS) information resources in accordance with applicable state and federal laws, rules, and regulations.
ePHI	**Electronic Personal Health Information** An electronic version of demographic information, medical history, test and laboratory results, insurance information, and other data that is collected by a health care professional to identify an individual and determine appropriate care.
ESB	**Enterprise Service Bus** Provides services and communication between applications in the TIERS middleware layer.
EWS	**Enterprise Web Services** Provides services and communication between applications in the TIERS middleware layer.
FERPA	**Family Educational Rights and Privacy Act** A federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
FIPS	**Federal Information Processing Standards** A publicly announced standardization development by the U.S. federal government for use in computer systems.
FISMA	**Federal Information Security Management Act of 2002** Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
FTI	**Federal Tax Information**

Acronym / Term	Description
	Any tax return or tax return information received directly or indirectly from the U.S. Secretary of the Treasury.
HHS	**Health and Human Services** A Texas system composed of five agencies that operate under the oversight of the Health and Human Services Commission
HHSC	**Health and Human Services Commission** Oversees the operations of the health and human services system, provides administrative oversight for Texas health and human services programs and directly administers some programs.
HIPAA	**Health Insurance Portability and Accountability Act of 1996** Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.
HITECH	**Health Information Technology for Economic and Clinical Health** Enacted as part of the American Recovery and Reinvestment Act of 2009, HITECH was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
HTTP	**Hypertext Transfer Protocol** The underlying protocol used by the World Wide Web to define how messages are formatted and transmitted.
HTTPS	**HyperText Transfer Protocol Secure** A protocol for secure communication over computer networks, widely used on the Internet.
IDS	**Intrusion Detection System** A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.
IM&O	**Infrastructure Management & Operations** A department of HHSC that manages shared services and assets that support HHS agencies (HHSC, DADS, DARS, DFPS, DSHS).
IPS	**Intrusion Prevention System** A system designed to actively monitor and prevent malicious software/intrusions on the network, and send alerts to administrators.
ISSO	**Information System Security Officer** Individual with responsibility for agency-wide information security, information security performance reporting, compliance with federal security laws, regulations, guidance, audits, and security compliance reviews.
Key Escrow	**Key escrow** is a method of storing important cryptographic keys. Each key stored in an escrow system is tied to the original user and subsequently encrypted for security purposes.
LDAP	**Lightweight Directory Access Protocol**

Acronym / Term	Description
	Protocol for querying and modifying items in directory service providers like Active Directory.
MARS-E	**Minimum Acceptable Risk Controls for Exchanges** NIST-based framework developed by CMS to facilitate compliance with the security requirements for Exchange and common program enrollment systems.
MDCN	**Medicare Data Communications Network** A secure closed private network currently used to transmit data between Medicare fee-for-service (FFS) contractors and the Centers for Medicare and Medicaid Services, as well as for transmission of electronic transactions in some cases from certain providers and clearinghouses to FFS contractors.
MPLS	**Multiprotocol Label Switching** A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.
NARA	**National Archives and Records Administration** An independent agency of the U.S government charged with preserving and documenting government and historical records.
NAS	**Network-attached storage** Computer data storage server connected to a computer network providing data access to a heterogeneous group of clients.
NIST	**National Institute of Standards and Technology** A federal technology agency that works with industry to develop and apply technology, measurements, and standards.
NTP	**Network Time Protocol** Networking **protocol** for clock synchronization between computer systems.
NVD	**National Vulnerability Database** A U.S. government online repository of standards-based vulnerability management data, operated by NIST.
OIG	**Office of the Inspector General** The IG works to prevent, detect, and pursue fraud, waste, and abuse in the Texas Health and Human Services system.
OMB	**Office of Management and Budget** An agency of the Executive Office of the President of the United States.
PCI DSS	**Payment Card Industry Data Security Standard** Provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.
PDA	**Personal Digital Assistant** A mobile device that functions as a personal information manager.
PHI	**Personal Health Information** Also referred to as protected health information, generally refers to demographic information, medical history, test and laboratory results,

Acronym / Term	Description
	insurance information, and other data that is collected by a health care professional to identify an individual and determine appropriate care.
PII	**Personally Identifiable Information** Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
PIN	**Personal Identification Number** A secret numeric password shared between a user and a system that the system uses to authenticate the user.
POA&M	**Plan of Action and Milestones** A document that identifies tasks to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for completing the tasks, and scheduled completion dates for the milestones.
RA	**Risk Assessment** The evaluation of potential vulnerabilities in order to protect information systems from threats.
SANS	**System Administration, Networking, and Security Institute** The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. SANS is the most trusted and by far the largest source for information security training and security certification in the world.
SAR	**Safeguard Activity Report** An annual IRS-required report from agencies that advises the IRS of minor changes to the procedures or safeguards described in the Safeguard Procedures Report (SPR).
SCSEM	**Safeguard Computer Security Evaluation Matrix** Security evaluation templates produced by the IRS and publicly available.
SDC	**Service Delivery Center** A single sign-on application where HHSC staff initiate tasks or work assignments, launch TIERS, view images and schedules, record complaints/ requests for fair hearings and perform other activities related to eligibility determination.
SDLC	**System Development Life Cycle** The overall process of developing information systems using a multistep process.
SFTP	**Secure File Transfer Protocol** Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream.
SNAP	**Supplemental Nutrition Assistance Program** Helps people buy the food they need for good health. SNAP offers nutrition assistance to eligible, low-income individuals.
SOW	**Statement of Work**

Acronym / Term	Description
	A formal document that captures and defines work activities, deliverables, and timelines for a project. Standard regulatory and governance terms and conditions are included.
SOX	**Sarbanes-Oxley Act of 2002** An act passed by U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations. The Sarbanes-Oxley Act mandated strict reforms to improve financial disclosures from corporations and prevent accounting fraud.
SPR	**Safeguard Procedures Report** An IRS-required report that describes the procedures established and used by an agency for ensuring the confidentiality of information received from the IRS.
SSH	**Secure Shell** A UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.
SSL	**Secure Sockets Layer** A standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. Superseded by TLS.
SSP	**System Security Plan** A formal plan that provides an overview of the security requirements of a system. It describes the controls in place or planned and the responsibilities and expected behavior of all individuals who access the system.
SSP	**Self Service Portal** The Self-Service Portal is available to clients 24 hours a day, 7 days a week. They can use this website to check the status of documents submitted to HHSC, submit applications, submit redeterminations, report changes, check the status of their benefits, and check future appointments.
STP	**State Portal** Built for call center to search and view documents, cases, individuals, benefits, and other facts about eligibility.
ST&E	**Security Testing and Evaluation** A means of determining or verifying that information security controls are operational, adequate, and effective in preventing inadvertent or deliberate disclosure, alteration, or destruction of agency information and resources.
TAC	**Texas Administrative Code** A compilation of all state agency rules in Texas.
TANF	**Temporary Assistance for Needy Families** TANF helps families pay for basic living needs.
TFC	**Texas Facilities Commission** A state agency responsible for planning, providing, and managing facilities for state agencies.
TIERS	**Texas Integrated Eligibility Redesign System**

Acronym / Term	Description
TIGTA	**Treasury Inspector General for Tax Administration** This United States agency provides independent oversight of IRS activities.
TLM	**Task List Manager** A Service Delivery Center application that manages tasks for HHSC staff. Staff select tasks based on workload availability or assignment.
TLS	**Transport Layer Security** A protocol that ensures privacy between communicating applications and their users on the Internet. TLS is the successor to the Secure Sockets Layer (SSL).
TSP	**Telecommunications Service Priority** Established by the Federal Communications Commission (FCC), TSP is a regulatory, administrative, and operational framework that authorizes national security and emergency preparedness organizations to receive priority treatment for vital voice and data telecommunications services.
VLAN	**Virtual Local Area Network** A logical grouping of network nodes.
VoIP	**Voice over Internet Protocol** A family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
VPN	**Virtual Private Network** A network that uses primarily public telecommunications infrastructure, such as the Internet, to provide remote offices or traveling users' access to a central organizational network.
WAF	**Web Application Firewall** A firewall that monitors, filters or blocks the HTTP traffic to and from a Web application.
WDC	**Winters Data Center** Primary data center for Texas HHS.
Workload	Workload is the amount of processing that a (physical or virtual) server is given to do at a given time. The workload consists of some amount of application execution on the server and some number of users interacting with the server's applications.
YTB	**Your Texas Benefits** The Self-Service Portal available to clients 24 hours a day, 7 days a week. YTB is also a mobile app.

Attachment B: TIERS and EST Applications Overview

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Table of Contents

1. TIERS Ecosystem 3
2. TIERS Module 5
3. YourTexasBenefits.com (YTB) / Self-Service Portal (SSP) 6
4. Long Term Services and Support (LTSS) - Screener 9
5. LTSS Worker Portal 11
6. Mobile Application 13
7. HHSC Lightweight Enterprise Application Platform (LEAP) 13
8. HHSC Agile Dashboard Tool 15
9. TIERS and EST Applications - Technical Tools 21

1. TIERS Ecosystem

The TIERS Ecosystem consists of numerous integrated interrelated applications and business functions. The technical aspect of the TIERS system consists of a collection of information systems spanning multiple platforms. These systems include the TIERS and Eligibility Supporting Technologies (EST) applications.

Table 1: TIERS Ecosystem & Environment

System Environment	Description
System Owner	The TIERS information system is owned by the State of Texas
System Operation	TIERS is operated by a combination of state employees and contractors.
System Support Services	— Winters Data Center Operations – currently operated by Northrup Grumman (NG) — San Angelo Data Center Operations – currently operated by Atos, Northrup Grumman (NG) — Network – currently operated by Insight Networking — TIERS System Applications – currently operated by HHSC and Deloitte — Call Centers – currently operated by MAXIMUS — Public Benefits Offices – operated by HHSC
User Accounts, Account Organizations Active Users	User Account Type / Organizations / Est. Active Users TIERS / HHSC / 19,000 State Portal / HHSC / 16,000 DataMart / Deloitte, HHSC / 9,000 CCI (Call Center Inquiry) / MAXIMUS / 1,600 Self-Service Portal / Clients / 4,700,000
Critical Processing Periods	Critical processing periods vary depending on the component, but most notably for the user facing web interfaces occurs between 10:00 A.M. and 2:00 P.M. The critical processing period for the batch process is scheduled to occur overnight from 8:30 P.M. to 7:00 A.M.
Offsite User Organizations and Types	To make it easier and more efficient for Texans to apply for and manage their state benefits, the Texas Health, and Human Services Commission (HHSC) partners with Community Based Organizations (CBO) to help people learn how they can get the most out of the HHSC's benefits application and management website, YourTexasBenefits.com. The organizations that become Community Partners represent a wide range of social services, including public entities, non-profit organizations, and faith-based groups. CBOs assist applicants filing for benefits. Authorized contracted CBOs may perform SNAP interviews. Public Benefits offices are located throughout the State of Texas and staffed by state employees. These offices support face-to-face interaction with clients.

Table 1: TIERS Ecosystem & Environment

Table 2: TIERS & EST Applications and Business Functions		
Name	**Acronym**	**Business Function**
Texas Integrated Eligibility Redesign Systems	TIERS	The TIERS Core component (comprising TIERS Online, TIERS Batch, LUW Web Services, and TIERS database) includes a central data repository to collect eligibility information, a web interface, interfaces with other systems, decision table logic to process information and determine eligibility, and client notice generation.
Your Texas Benefits Self Service Portal (SSP)	YourTexasBenefits.com (SSP)	The Your Texas Benefits online portal is available to clients 24 hours a day, 7 days a week. Applicants can use this website to check the status of documents submitted to HHSC, submit applications, submit redeterminations, report changes, check the status of their benefits, and check future appointments.
Your Texas Benefits Mobile Application	Mobile App	A mobile application for people in Texas who have applied for or get SNAP food benefits, health-care benefits such as Medicaid and CHIP, or TANF. The mobile application is available on the iOS and Android platforms. The application supports many functions including: create a new account, upload supporting documents, view notices and reminders, submit change requests, locate nearby HHSC offices, check the status and amount of benefits, and receive renewal notifications.
Long-Term Services and Supports	LTSS Screener LTSS Worker Portal	Includes two applications, a pre-screener and referral app that supports Texans with determining if they qualify for support services and should complete a full application, and referral based on the screener app outcome.
State Portal / Service Delivery Center	STP/ SDC	A single sign-on application where HHSC staff initiate tasks or work assignments, launch TIERS, view images and schedules, record complaints/ requests for fair hearings and perform other activities related to eligibility determination.
Scheduler	Scheduler	A State Portal application that schedules and reschedules appointments for application, expedite, or redetermination interviews.
Task List Manager	TLM	A State Portal application that manages task workflow for state and vendor eligibility workers. Staff select tasks based on workload availability or assignment. The TLM Global Queue and TLM Personal Queue are used to receive and monitor activities and due dates. The user role determines the tasks staff can view.
Call Center Inquiry	CCI	The Call Center Inquiry application assists customer service representatives in rapidly collecting TIERS information on a specific client or case.
Document Center	Doc Center	Document Center is an HHSC-owned application developed to support the vendor staff involved in pre-processing of documents received through channels: Mail, Fax, SSP, and Call Center. Pre-processing of documents includes but not limited to: classification, association to a TIERS case, and routing of a document to state staff for further processing

Table 2: TIERS & EST Applications and Business Functions		
Name	**Acronym**	**Business Function**
DataMart Reports	DataMart	DataMart is a reporting system that pulls data from TIERS, TLM, STP and SSP. It then presents a set of operational reports to let TIERS users and management know the status of various activities in the system.
Enterprise Content Manager	ECM	The TIERS Enterprise Content Manager provides the content and document management system for TIERS. All images of case and client related documents including incoming mail, incoming fax, and outgoing correspondence, notices and forms from all eligibility systems are stored and managed in a single system of record.
Community Based Organizations Portal	CBO Portal	The CBO Portal is an enhanced version of the Self-Service Portal that provides additional functionality for CBO staff. This enhanced functionality is enabled based on CBO login to the Self-Service Portal (SSP), also known as YourTexasBenefits.com.

2. TIERS Module

The Texas Integrated Eligibility Redesign System (TIERS) and supporting technologies are designed to automate and support eligibility determination for HHSC Enterprise programs TIERS is the system of record and the primary system responsible for supporting the administration and management of HHSC programs in Texas. Together with other supporting technologies, TIERS is used to process applications and determine eligibility for various HHSC public assistance programs and support other functions of the HHSC office of access and eligibility services. TIERS serves as the technological foundation of the Texas Health and Human Services Commission's efforts to modernize its eligibility system.

TIERS automate the processing of a complex set of rules applied to ensure consistency in eligibility determination. TIERS also integrates technologies (e.g., bar codes) and integrates external data sources (e.g., income verification) to reduce the need for repetitive data-entry tasks. TIERS and EST Applications bring several advantages to the State: improved customer service, expanded access to services without expanded paperwork, a more efficient platform for workers, enhanced fraud protection tools, and flexible technology adapting to changes in policy or law.

TIERS is a web-enabled application built using J2EE (Java Enterprise Edition) and WebSphere Application Server technologies. These technologies provide the technical foundation to enable and evolve the multi-channel client interaction business model for HHSC.

Core TIERS assets including the database, rules engine, and application modules for face to face process automation are currently in production and effectively support case processing. TIERS capabilities are effectively integrated with YourTexasBenefits Self Service Portal (yourtexasbenefits.com), YourTexasBenefits mobile app, and other

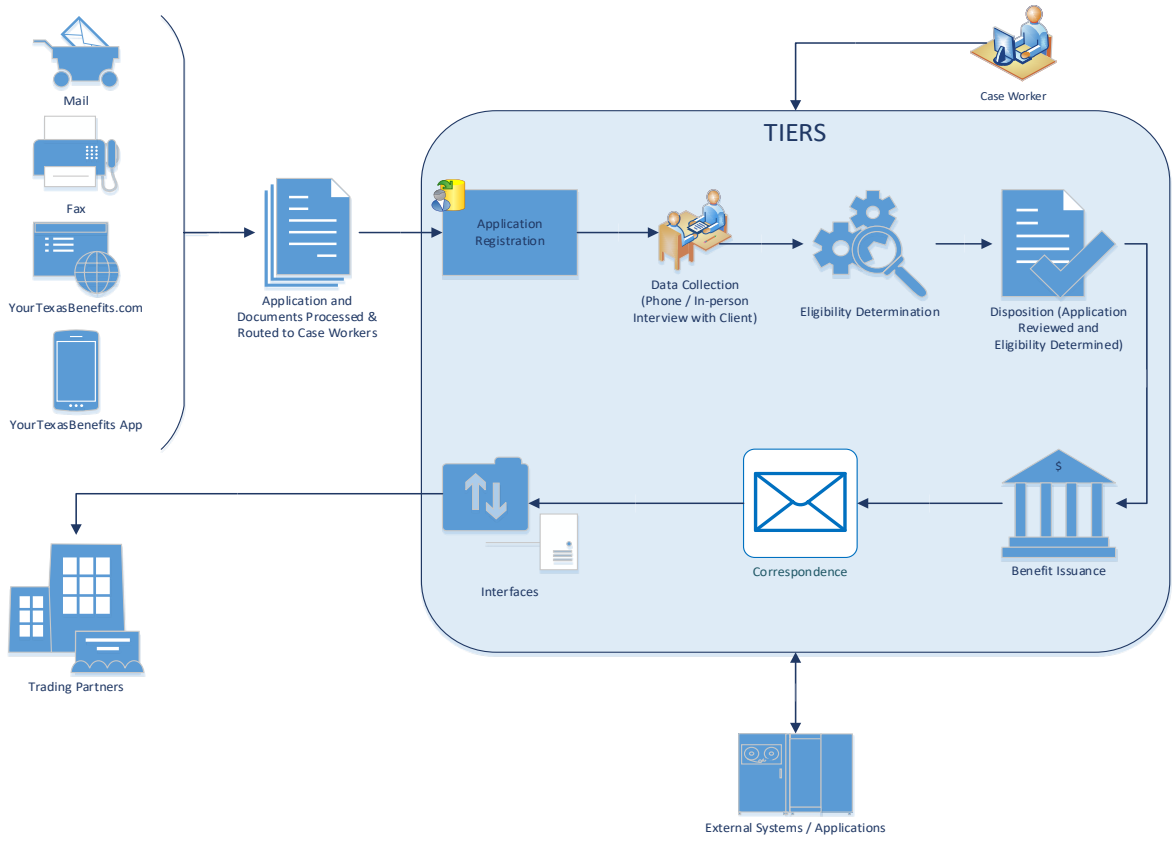
eligibility supporting technologies using a Services Oriented Architecture (SOA) approach.

TIERS architecture supports delivering online services to users and batch services to other peripheral systems. Different commercial and custom developed components make up this architecture. A Java based framework forms the basis of the TIERS application. Frameworks in TIERS are classified as core and common. Core services are framework abstractions and mechanisms built around standard industry Java and J2EE patterns. Core services are composed of presentation, business, persistence, and batch subsystems. Each of these subsystems has abstractions and coarse-grained interfaces that decouple the application from frameworks.

TIERS technologies provide the technical foundation to enable and evolve the multi-channel client interaction business model for HHSC. Core TIERS assets include the database, rules engine, and application modules for automation currently in production and, effectively support face-to-face case processing.

A high-level description of the TIERS related business processes is provided in the following figure.

Figure 1: TIERS Business Process



3. YourTexasBenefits.com (YTB) / Self-Service Portal (SSP)

YourTexasBenefits.com, also known as Self-Service Portal (SSP), is the HHS website developed to help Texas citizens in need of assistance. Clients learn about, apply, renew, and report changes for the following services, including:

1. **SNAP food benefits** - Helps families buy healthy food.
2. **TANF Cash Help** - Helps families with children age 18 and younger pay for basic needs.
3. **Health Care -** Helps cover visits to doctors, dentists, and hospitals. Also covers medicines ordered by Doctors and Dentists.
4. **Support Services** - Helps people with daily living needs, caregivers, and people with mental health, drug, or alcohol problems.

Clients currently have access to the following website features:

- Set up a new account
- View basic case facts and status
- View files and forms sent to HHSC
- Apply for or renew benefits
- Report and submit changes
- See all history or previous benefits
- View/Print Temporary Medicaid ID Card
- Choose to go paperless
- View letters and forms from HHSC
- Sign up for alerts
- Upload documents and images

YourTexasBenefits.com is a large-scale, widely used, web-based. The website averages over one million logins per month and processes approximately three million transactions per day.

YourTexasBenefits.com promotes improved business processes and increases efficiency for the State.

1. Efficiencies are gained by reduced data entry, automated verifications, and other automated processes.
2. Allows State staff and State Trading Partner staff to focus on core functions – determining eligibility and verifying information submitted.
3. Self-service options are less costly than call centers.
4. Documents can be uploaded directly to HHSC, reducing imaging costs.
5. Mail costs can be reduced by delivering client notices electronically.
6. Reductions in workload can result in less State staff overtime.
7. Printing and imaging costs are reduced.

YourTexasBenefits.com provides effective and efficient alternatives to client and reduces visits to eligibility offices and calls to 2-1-1 contact center.

Texas citizens rely heavily on YourTexasBenefits.com to swiftly apply for benefits and check status on their accounts.

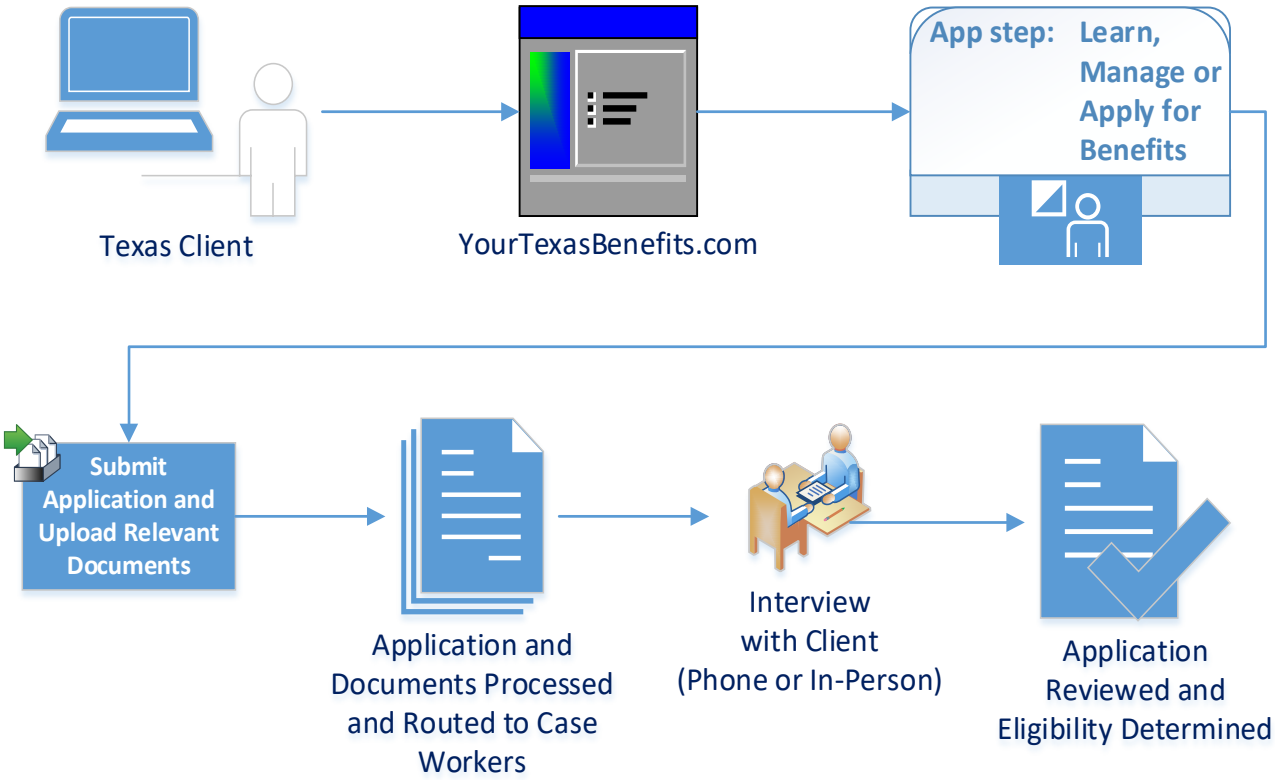
The YourTexasBenefits.com design and architecture was modernized in August 2015. The new applications architecture strategy was based on HHSC's Lightweight Enterprise Application Platform (LEAP). The modernization project was developed to meet the following objectives:

1. Simple workflows easily understood by clients
2. Ease of navigation when interacting with the website
3. Full American Disability Act (ADA) compliance
4. Sub-second response times
5. Architecture simplicity
6. Leverage widely used and secure open source components
7. Layered architecture, separating the presentation and business layers
8. Service Oriented Architecture (SOA)

The website is divided into three (3) sections: Learn, Apply, and Manage. It provides a Messaging Center, Help Topics, and a robust search engine for answering client questions. The workflow process is easy to understand and provides a progress bar as the client navigates seamlessly through screens.

The YourTexasBenefits.com business process begins with the client in need of services or information visiting the website. The following diagram depicts the high-level process when a person selects the APPLY tab on the website and concludes with eligibility determination for requested services achieved. The application process is easy to navigate through and begins the process of applying for, and learning about, the services HHS agencies offer.

Figure 2: YourTexasBenefits.com Business Process (SSP)



4. Long Term Services and Support (LTSS) - Screener

Federal law established the Balancing Incentive Program (BIP) to make certain structural reforms to increase funding and access to Medicaid community-based LTSS.

Texas has a lengthy history of promoting the independence of clients and re-directing their services to home based long term care versus institutional nursing facility care. The State has a successful "Money Follows the Person Demonstration program (MFP Demonstration)" that helps individuals residing in nursing facilities and intermediate care facilities transition and relocate to the community and receive home and community based services. In addition, the State has a strong network of Aging and Disability Resource Centers (ADRCs) from which to establish a fully “no wrong door/single entry point” LTSS eligibility system.

HHS implemented both programmatic and automation structural changes under the Balancing Incentive Program (BIP) grant in 2015 to increase the percentage of clients using community based services. The primary automation change was creation of both a LTSS Screener and an LTSS Worker Portal and an LTSS Citizen Portal.

Clients can access the LTSS Screener through YourTexasBenefits.com. Depending on answers clients provide in the Screener, they will be presented a summary of the benefits and services they might be able to obtain.

Potential LTSS clients include:

1. People who are older or have a disability
2. People who are caring for a person who is older or has a disability
3. People who need help with a mental health issue
4. People who need help with drug or alcohol abuse issues

The possible LTSS services include the following:

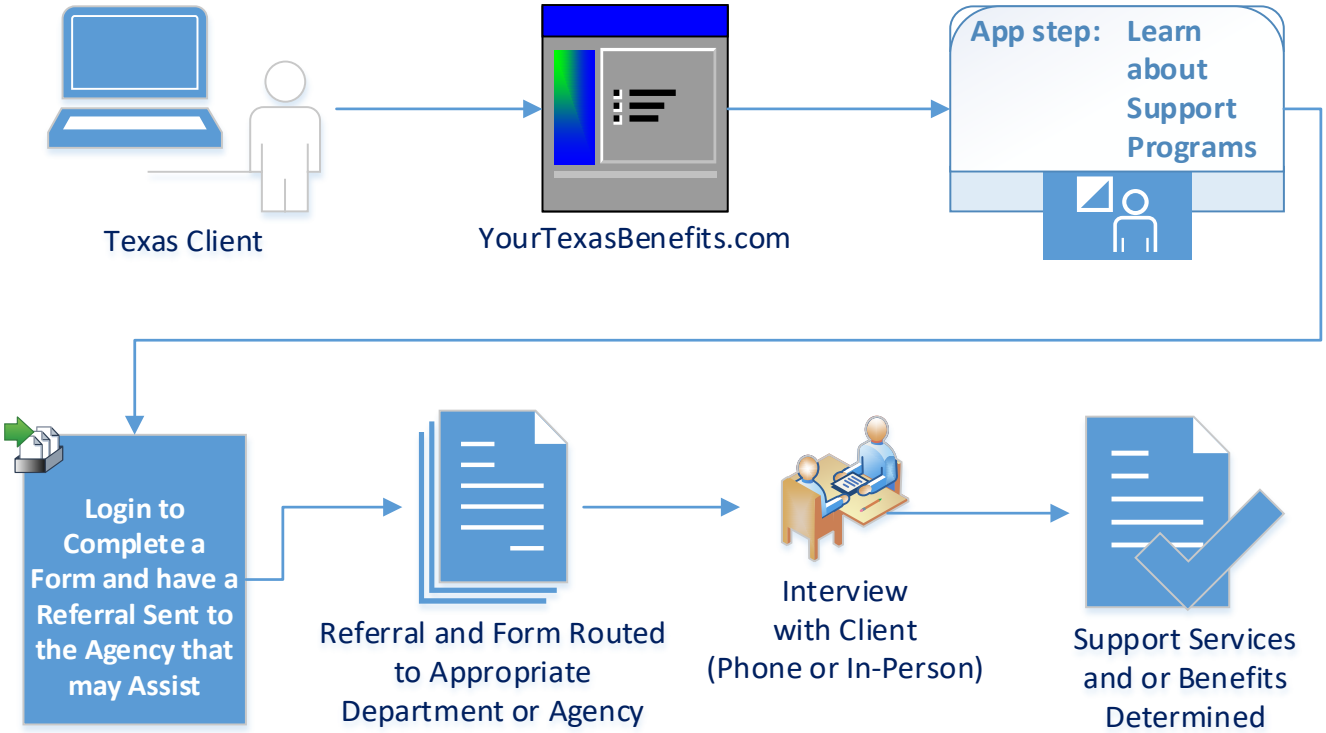
1. Help with daily living needs, such as bathing, dressing, eating, shopping, laundry, or making meals
2. Help for caregivers who need a short break (respite services)
3. Treatment for mental health issues
4. Treatment for drug or alcohol abuse issues

The Long-Term Services and Support (LTSS) Screener provides the following features:

1. Navigate to YourTexasbenefits.com
2. Review support programs
3. Create an account and login
4. Complete questionnaire
5. Submit referral form

The LTSS Screener business process is summarized below:

Figure 3: LTSS Client Screener Business Process

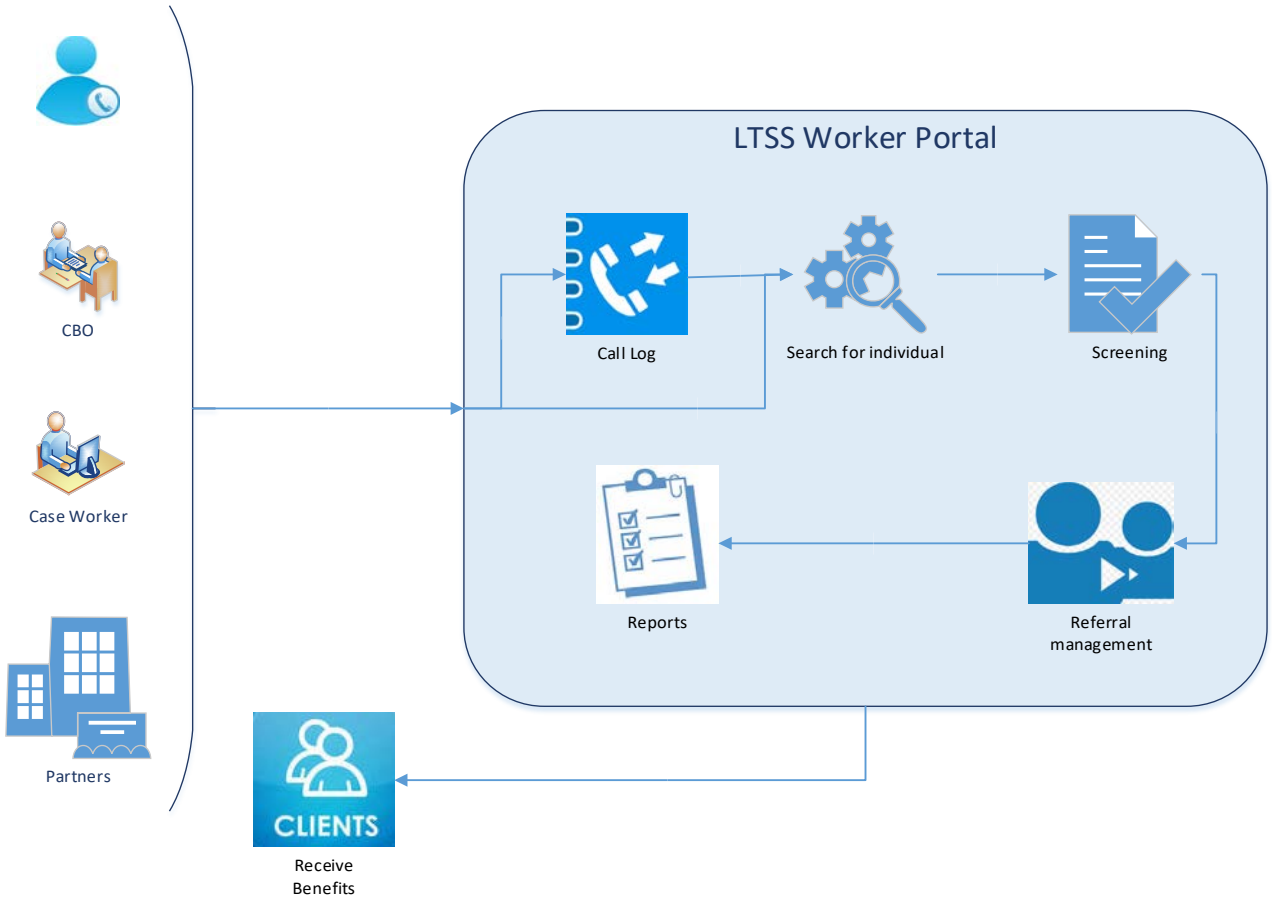


5. LTSS Worker Portal

The LTSS Worker Portal provides end users (workers) from all LTSS entities the ability to record client contacts and to perform a high-level LTSS screening and referral management procedures. Additionally, the LTSS Worker Portal supports sharing of information between various State entities to facilitate assisting individuals interested in receiving LTSS services and support. The business process for the LTSS Worker Portal is summarized in the diagram below. Key features of the Portal are:

1. LTSS Search - provides the capability to search for LTSS screenings, referrals, and related information for an individual.
2. Referral Management - provides the capability for an end user to perform referral management.
3. Reporting - provides the capability for an end user to generate a LTSS Screening Report based on the role and parameters they specify.

Figure 4: LTSS Worker Portal Business Process



6. Mobile Application

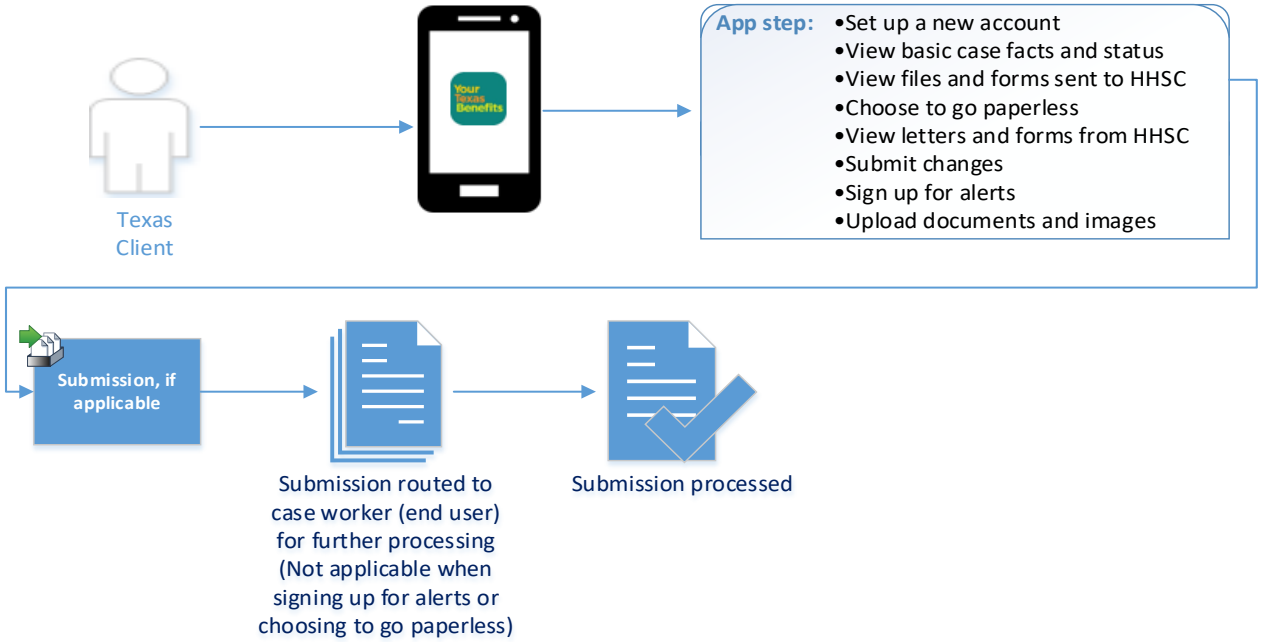
The Your Texas Benefits Mobile Application was developed for the citizens of Texas who have applied for or receive SNAP, Medicaid, CHIP, TANF, or other public assistance benefits. The App supports many functions including: create a new account, upload photos of supporting documents, view notices and reminders, submit change requests, locate nearby HHSC offices, check the status and amount of benefits, and receive renewal notifications. The Mobile Application compliments the YourTexasBenefits.com website, but does not replicate the website's complex business processes where clients apply, renew, and report all changes.

Currently the Mobile Application supports the Apple iOS and Google Android (with Google Mobile Services) operating systems. JavaScript is the programming language for Mobile Application and Java is the programming language used in the associated web services.

Clients access the Mobile Application by downloading and installing the app on their device through the Apple iTunes or Google Play application stores.

The Mobile App business process is summarized in the diagram below. If the client submits changes or uploads documents images, the submission is routed to a State case worker for further action. The case worker will take appropriate action on the case and complete the processing of the reported change or action. The Mobile Application will notify the client of the outcome.

Figure 5: Mobile Application Business Process



7. HHSC Lightweight Enterprise Application Platform (LEAP)

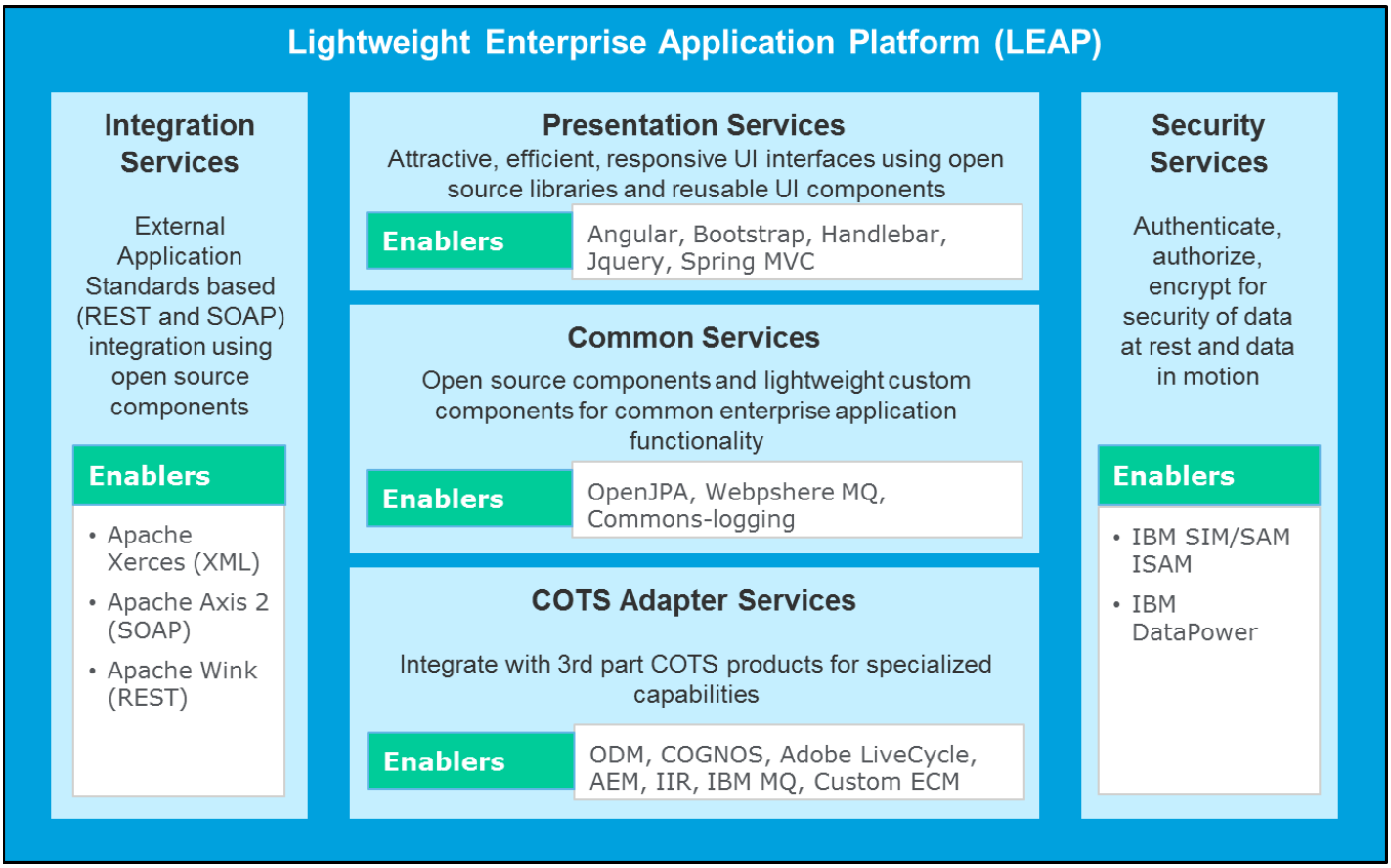
LEAP is HHSC's lightweight approach for designing and developing applications that uses architecture simplification as a core tenet to create high performance and scalable

applications with sub-second response times. The platform is implemented using proven modern open source and standards-based technologies. These technologies are widely used in the industry to build large commercial high volume, high transaction web applications. The platform avoids unwanted abstraction, rigid patterns and complex interactions leading to an approach that is easy to learn, develop, implement, and maintain.

This architecture was used for the modernization project for YourTexasBenefits.com. HHSC plans to convert additional applications in the TIERS and EST Applications to the LEAP platform in the future.

The diagram below highlights the key LEAP components:

Figure 6: LEAP Components



8. HHSC Agile Dashboard Tool

The Agile dashboard provides a single point of information sharing for all Agile stakeholders. The dashboard is a visualization tool that uses the power of analytics to aggregate data from multiple Agile tools and provide meaningful information to end users. It provides an easy way to track the details, progress and risks for projects and sprints.

The dashboard provides multiple views that present information pertinent to various roles and responsibilities in a consistent manner. The below table summarizes the various views and corresponding descriptions:

View Classification	Description
Functional Views	Provides views of Roadmap, Theme and Epics. These views are useful to Business and IT stakeholders, governance and HHS steering committee.
Development Views	Provides views of Cycle Set, Cycle, Sprint and Sprint Team. These views are useful to Business and IT stakeholders, scrum masters and sprint teams.
Deployment Views	Provides views of Risk and Release Management. These views are useful to Business and IT stakeholders, ACPs, Release Managers.

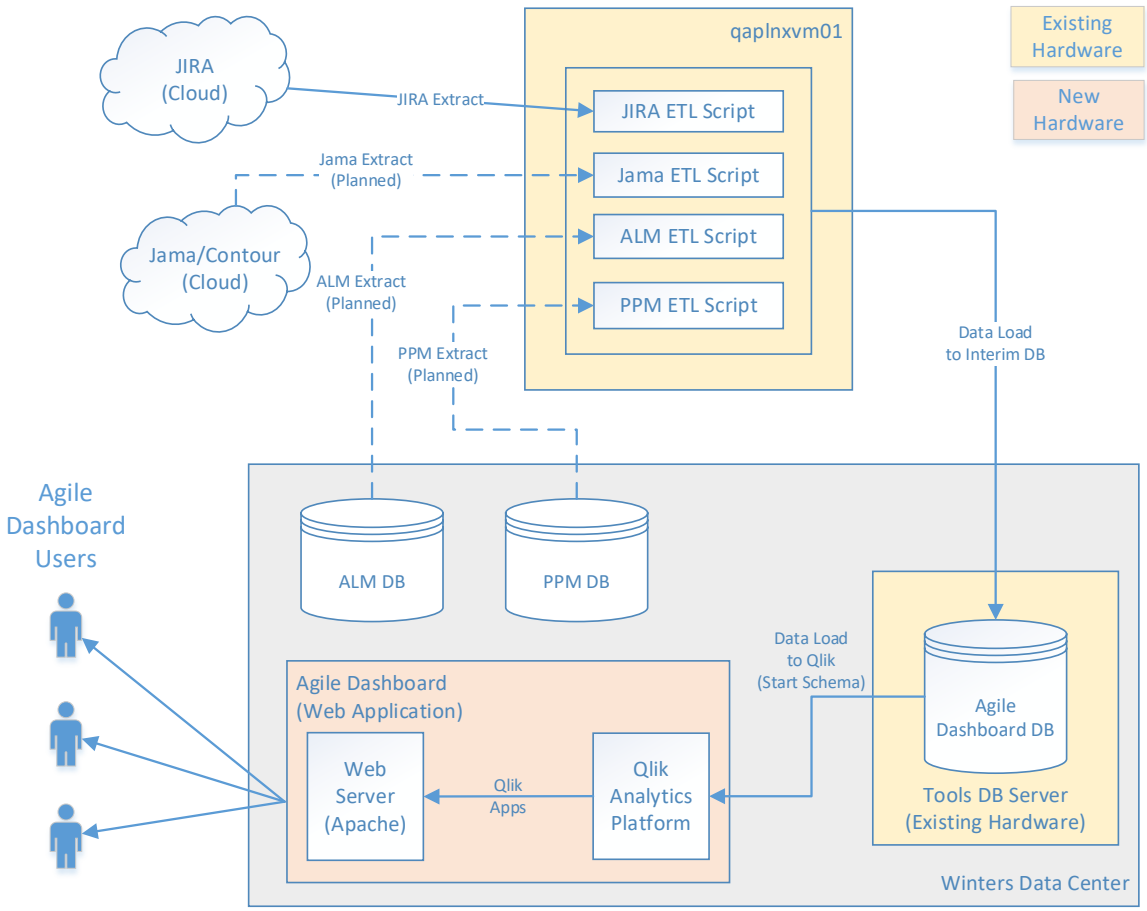
Technology Overview

Product and User Interface: The Agile dashboard is a responsive and highly interactive web application deployed in the Winters data center. The user interface theme is implemented using modern web standards such as *HTML5, CSS3, and Bootstrap responsive framework*. The Agile dashboard user interface is deployed on Apache web server and accessible to HHSC Intranet users over https using Secure Socket Layer (SSL).

The analytics capability is built on top of *Qlik Analytics Platform (QAP)*. The QAP applications are embedded in the web application as a mash-up to provide advanced data visualization using graphs, charts, tables and filtering capability. At the core of QAP analytics platform is Qlik Indexing Engine (QIX) which provides high performance in memory data processing and associative modeling for interactive dashboard features.

Data Extraction: The Extract Transform and Load (ETL) processes pull data from source systems such as JIRA at a regular interval and loads it in to Qlik's data warehouse in a star schema. The ETL processes can be extended to include other source systems such as Jama Contour (requirements management), HP Application Lifecycle Management (ALM) and HP Project and Portfolio Management (PPM).

Figure 7: Architecture Diagram for Agile Dashboard



Agile Dashboard Screenshots

The following pages include sample screen shots from the Agile dashboard. These are reflective of the various user experience patterns and views available in the application. The following sections also contain helpful hints to enable users to use the Agile Dashboard more effectively.

Expanding/collapsing the table rows to display/hide additional fields

The number of fields displayed and hidden in a table row adjusts dynamically depending upon the form factor and screen resolution.

Additional fields are collapsed and indicated with a '+' icon on the table row as shown in *Figure 8: Expand/Collapse table rows to display/hide fields.*

Click on the '+' icon to expand and view all the fields on the table row. Click the '-' icon on the expanded row to collapse it.

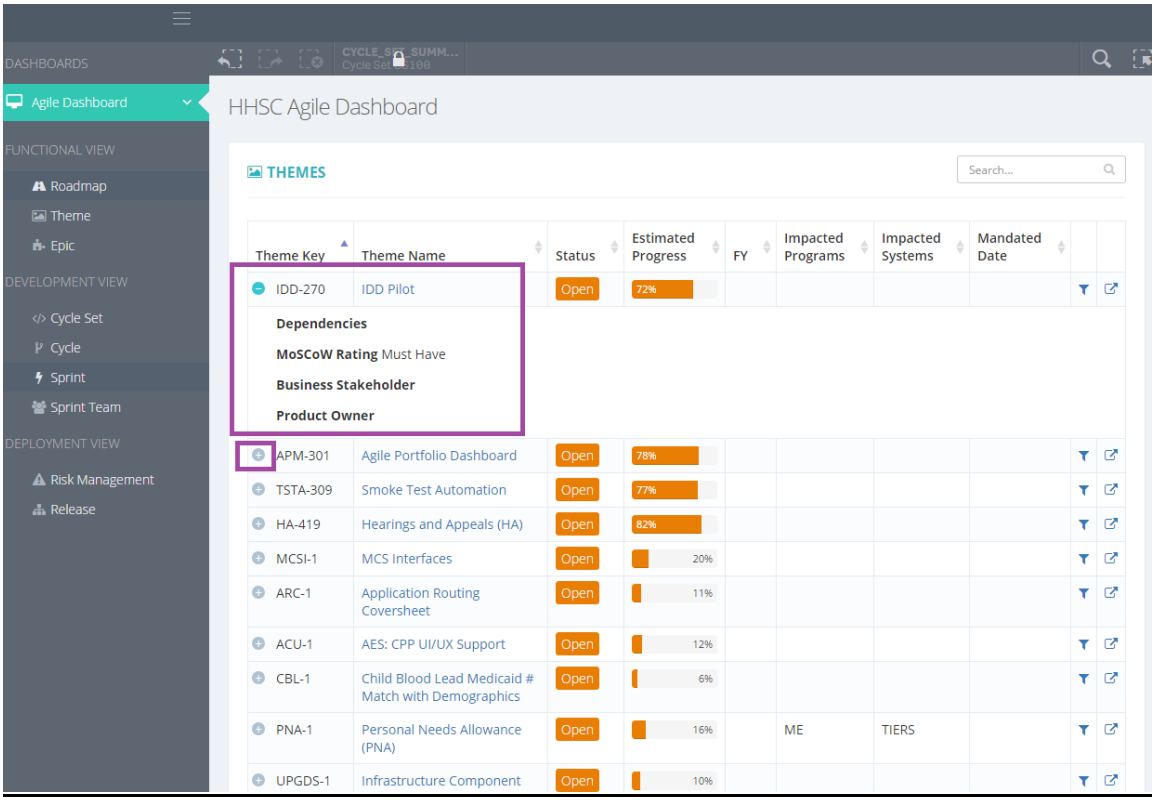


Figure8: Expand/Collapse table rows to display/hide fields

Unlocking default filters and selecting new filter values

The Agile Dashboard has a default filter set to the current cycle set. This is shown as a locked filter in the header menu bar as shown in *Figure 9: Unlock default filter*.

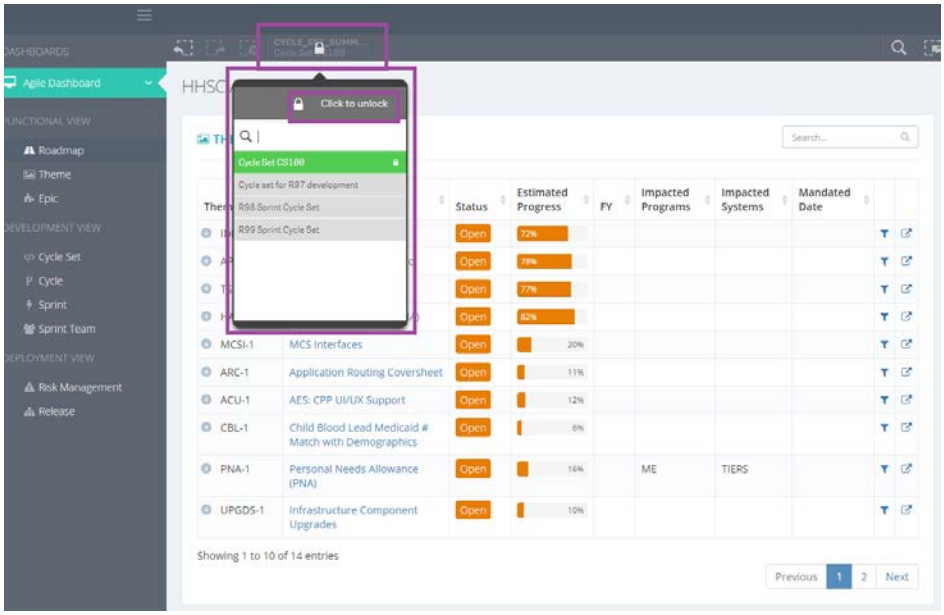


Figure 9: Unlock default filter

To select a new filter click on *"Click to unlock"* in *Figure 9: Unlock default filter* and select the desired filter criteria as shown in *Figure 10: Select default filter criteria*.

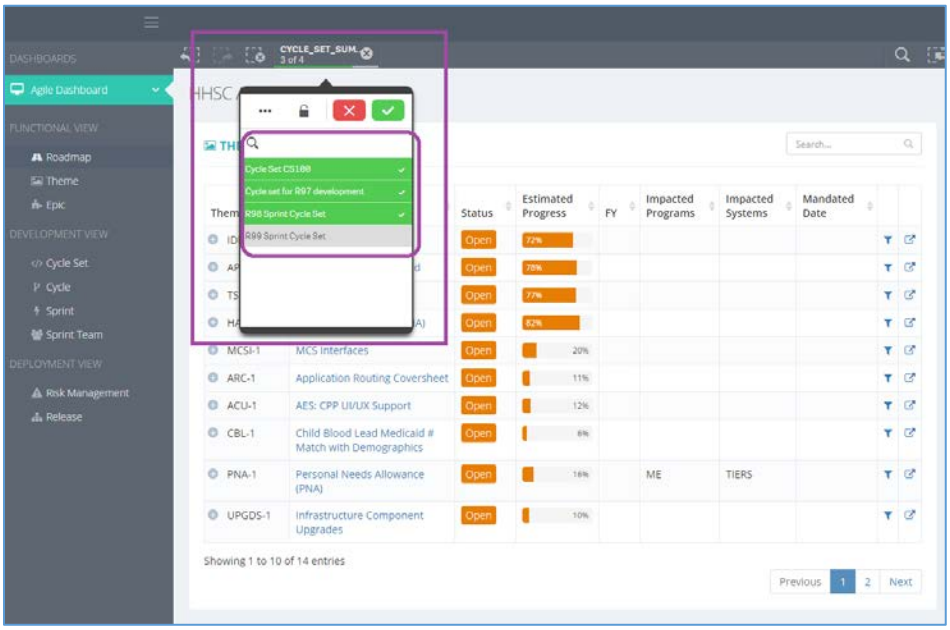


Figure 10: Select default filter criteria

Selecting filters and removing selected filters

Agile dashboard presents many different selection filters while selecting pie-charts, row filters and drop-down filters.

An example of Pie Chart Filter is shown in *Figure 11: Filter by selecting segments of pie charts*.

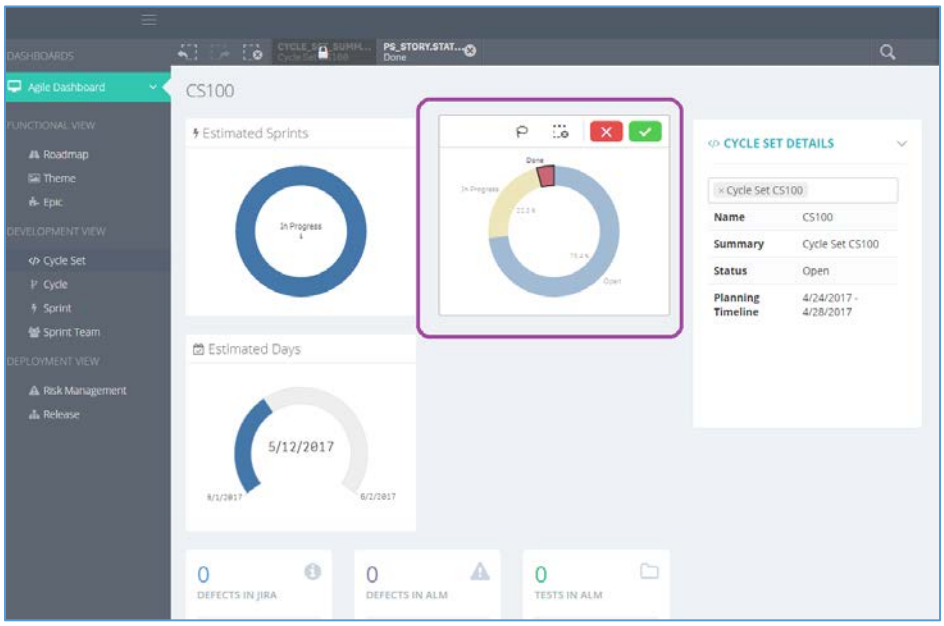


Figure 11: Filter by selecting segments of pie charts

An example of a row-filter is shown in *Figure 12: Filter by rows*

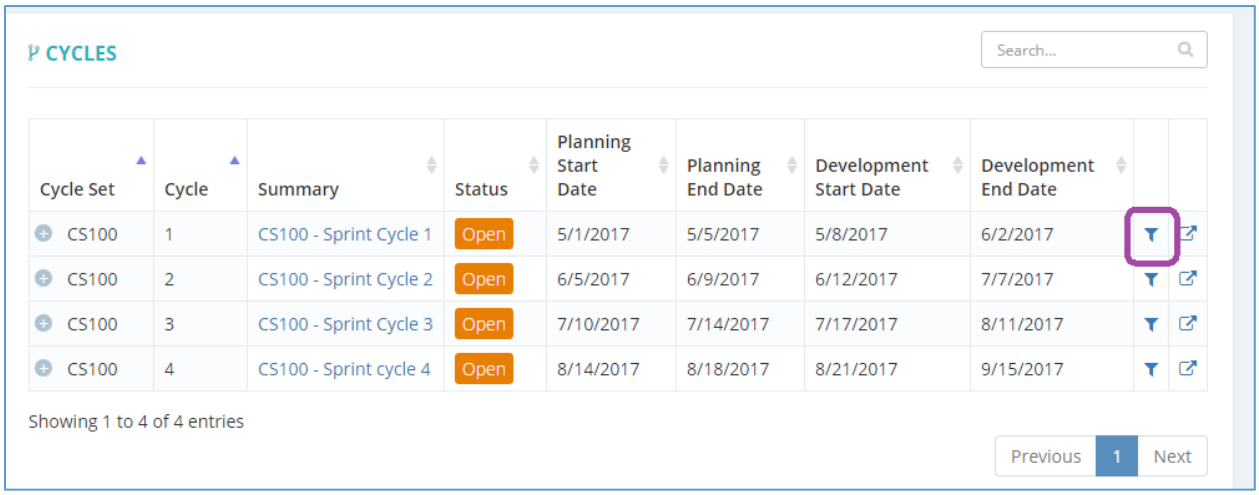


Figure 12: Filter by rows

An example of drop-down filter is shown in *Figure 13: Drop-down filter*

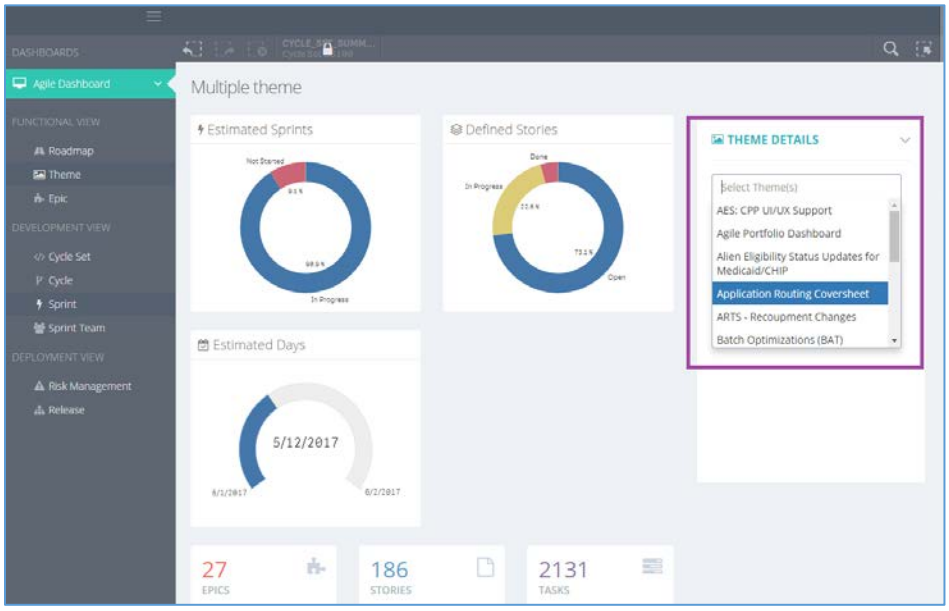


Figure 13: Drop-down filter

Values can be added or removed from a drop-down filter by selecting/removing values in the drop-down.

Filter selections can also be cleared from the header menu by **closing opened filters in the header** or selecting the ***"Clear all selections"*** icon in the header menu as shown in *Figure 14: Add/Remove values from Drop-down filter*

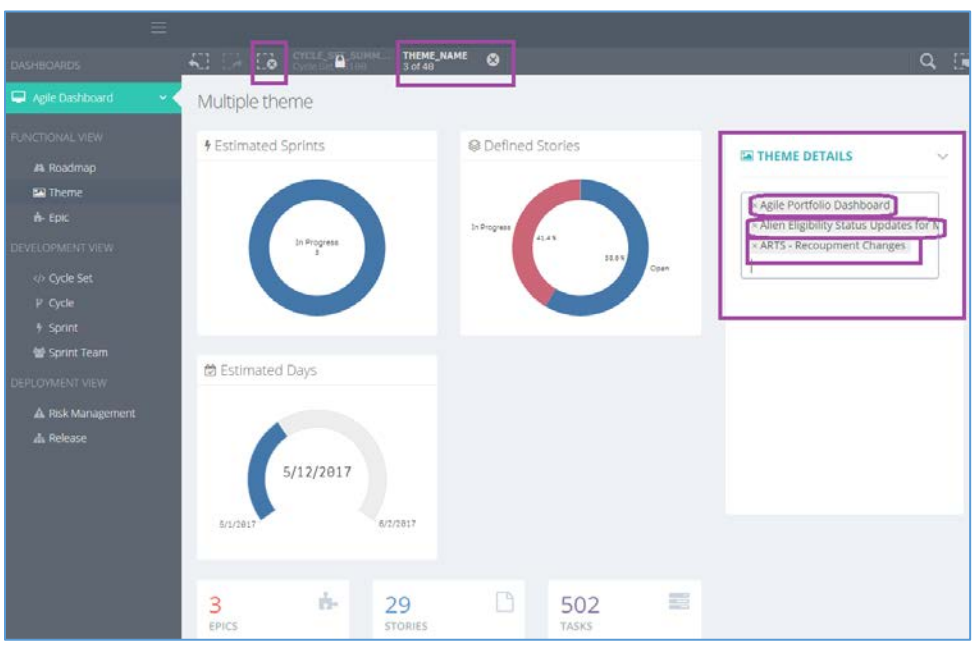


Figure 14: Add/Remove values from Drop-down filter

Navigating to JIRA

Users can navigate to JIRA to view the corresponding JIRA objects for all entities in the Agile dashboard by clicking on the pop-out icon in the corresponding table row. The users will be

prompted to login to JIRA for the first time and subsequently will not be prompted for login until the JIRA session expires.

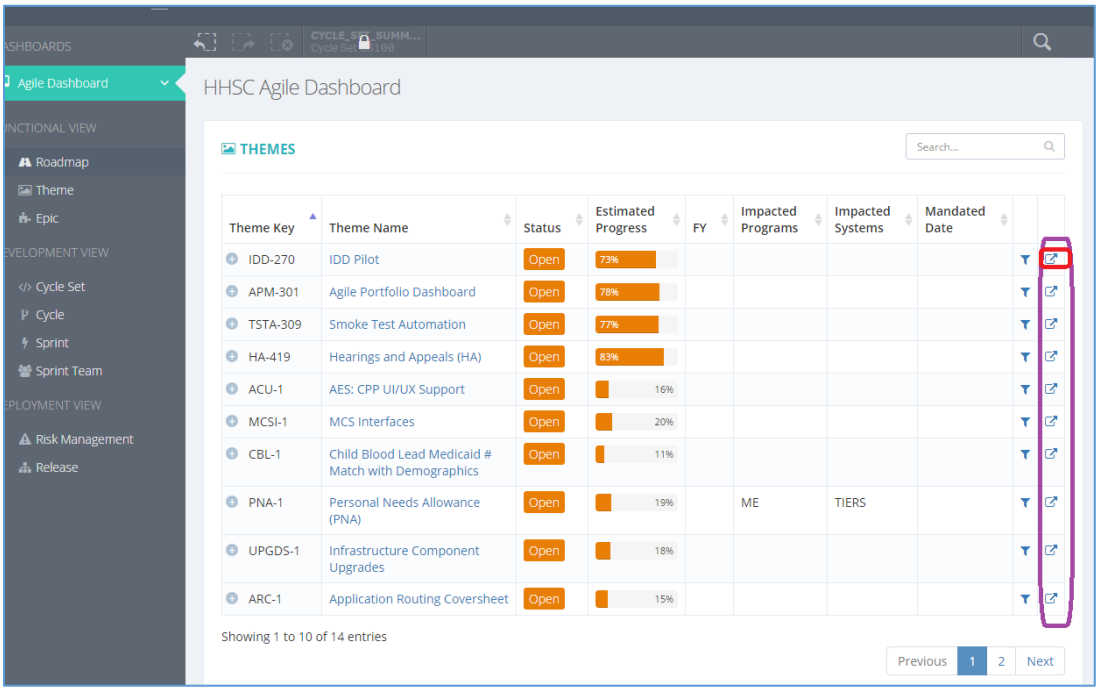


Figure 15: Navigating to JIRA

1. **Search table level data using 'Search' filters**

Every table has an associated 'Search' text box as shown in *Figure 16: Search table level data* where a user can enter search key words and filter the table to display rows pertaining to the search criteria. Remove the Search criteria to restore the original table.

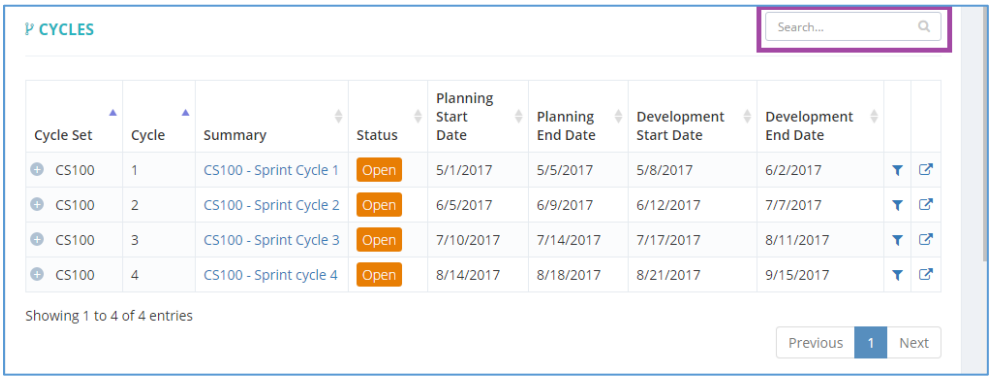


Figure 16: Search table level data

9. TIERS and EST Applications - Technical Tools

HHSC uses a variety of technical tools to support the TIERS Ecosystem. Table 4 summarizes the current tools that are employed.

Table 4: Technical Tools	
Tool	**Definition**
Adobe Experience Manager	Adobe Experience Manager is a tool that organizes, manages, and delivers creative assets. Its main purpose is to deliver relevant experiences to customers that will build brands, drive demand and facilitate outreach.
AngularJS	AngularJS, is an open-source web application framework mainly maintained by Google and by a community of individuals and corporations to address many of the challenges encountered in developing applications. It aims to simplify both the development and the testing of such applications by providing a framework for client-side model–view–controller (MVC) architectures, along with components commonly used in rich Internet applications.
Apache - Commons Logging (previously known as Jakarta Commons Logging (JCL)	Apache - Commons Logging (previously known as Jakarta Commons Logging (JCL), is a Java-based logging utility and a programming model for logging and for other toolkits. It provides APIs, log implementations, and wrapper implementations over some other tools.
Apache Axis2	Apache Axis2, is a core engine for Web services. It is a complete re-design and re-write of the widely used Apache Axis SOAP stack. Implementations of Axis2 are available in Java and C. Axis2 provides the capability to add Web services interfaces to Web applications. It can also function as a standalone server application.
Apache Wink	Apache Wink, is an open source framework that enables development and consumption of REST style web services.
Apache Xerces	Apache Xerces, is a collection of software libraries for parsing, validating, serializing and manipulating XML. The library implements a number of standard Application Programming Interface (APIs) for Extensible Markup Language (XML) parsing.
Bootstrap	Bootstrap, is a free and open-source collection of tools for creating websites and web applications. It contains HTML- and CSS-based design templates for typography, forms, buttons, navigation and other interface components, as well as optional JavaScript extensions. It aims to ease the development of dynamic websites and web applications. Bootstrap is a front end web framework, that is, an interface for the user, unlike the server-side code which resides on the "back end" or server.
CSS - Cascading Style Sheets	CSS - Cascading Style Sheets, is designed primarily to enable the separation of document content from document presentation, including aspects such as the layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple HTML pages to share formatting by specifying the relevant CSS in a separate .css file, and reduce complexity and repetition in the structural content.
Erwin Data Molder	Erwin is a data modeling software tool developed by erwin, inc. HHSC uses erwin to manage the database modeling, design, and related activities for TIERS and the related applications.
HandlebarsJS	HandlebarsJS, provides the power necessary to let you efficiently build semantic templates.

Table 4: Technical Tools	
Tool	**Definition**
HTML - HyperText Markup Language	HTML - HyperText Markup Language, commonly referred to as HTML, is the standard markup language used to create web pages. Along with CSS, and JavaScript, HTML is a cornerstone technology used to create web pages, as well as to create user interfaces for mobile and web applications.
IBM Cognos Business Intelligence	IBM Cognos Business Intelligence is a web-based, integrated business intelligence suite by IBM. It provides a toolset for reporting, analysis, score-carding, and monitoring of events and metrics. The software consists of several components to meet the different information requirements in a company.
IBM Operational Decision Management	IBM Operational Decision Management (ODM) is IBM's Business Rule Management System (BRMS). IBM ODM also incorporates IBM's implementation of Business Event Processing capabilities. IBM ODM can be installed both independently and as an application running on WebSphere Application Server.
Jama Connect	Jama Contour is a modern shared requirements management Platform for managing all requirements (versions, variants or from scratch), traceability, distributed team collaboration.
JASS - Java Authentication and Authorization Service	JASS - Java Authentication and Authorization Service, pronounced "Jazz", is the Java implementation of the standard Pluggable Authentication Module (PAM) information security framework. The main goal of JAAS is to separate the concerns of user authentication so that they may be managed independently. While the former authentication mechanism contained information about where the code originated from and who signed that code.
JavaScript	JavaScript, is a high-level, dynamic, un-typed, and interpreted programming language. It has been standardized in the ECMAScript language specification. Alongside PHP, HTML and CSS, it is one of the four essential technologies of World Wide Web content production; the majority of websites employ it and it is supported by all modern Web browsers without plug-ins.
JAXB - Java Architecture for XML Binding	JAXB - Java Architecture for XML Binding, allows Java developers to map Java classes to XML representations. JAXB allows storing and retrieving data in memory in any XML format, without the need to implement a specific set of XML loading and saving routines for the program's class structure.
JAX-RS - Java API for RESTful Web Services	JAX-RS - Java API for RESTful Web Services, is a Java programming language API that provides support in creating web services according to the Representational State Transfer (REST) architectural pattern. JAX-RS uses annotations, introduced in Java SE 5, to simplify the development and deployment of web service clients and endpoints.
JAX-WS - Java API for XML Web Services	JAX-WS - Java API for XML Web Services, is a Java programming language API for creating web services. JAX-WS is one of the Java XML programming APIs. It is part of the Java EE platform.

Table 4: Technical Tools	
Tool	**Definition**
JDBC - Java Database Connectivity	JDBC - Java Database Connectivity, is an application programming interface (API) for the programming language Java, which defines how a client may access a database. It is part of the Java Standard Edition platform, from Oracle Corporation. It provides methods to query and update data in a database, and is oriented towards relational databases.
Jenkins	Jenkins helps to automate the non-human part of the whole software development process, with common activities like continuous integration, but by further empowering teams to implement the technical part of a Continuous Delivery. It is a server-based system running in a servlet container such as Apache Tomcat.
JIRA	JIRA Software is an agile project management tool that supports any agile methodology, be it scrum, kanban, or any other unique flavor of Agile, developed by Atlassian. From agile boards to reports, one can plan, track, and manage all agile software development projects from a single tool, including bug tracking, issue tracking, and project management functions. HHSC uses this framework for the Agile Project Management.
JMS - Java Message Service API	JMS - Java Message Service API, is a Java Message Oriented Middleware (MOM) API for sending messages between two or more clients. JMS is a part of the Java Platform, Enterprise Edition. It is a messaging standard that allows application components based on the Java Enterprise Edition (Java EE) to create, send, receive, and read messages. It allows the communication between different components of a *distributed application* to be loosely coupled, reliable, and asynchronous.
JPA – Javap Persistence API specification	JPA – Javap Persistence API specification - The Java Persistence JSR-317 Java Persistence 2.0 standard is a Java Programming Interface Specification that describes the management of relational database in applications using Java Platform Standard Edition and Java Platform Enterprise Edition.
jQuery	jQuery - is a cross-platform JavaScript library designed to simplify the client-side scripting of HTML. jQuery is the most popular JavaScript library in use today, with installation on 65% of the top 10 million highest-trafficked sites on the Web.
Jrebel	JRebel is a Java development tool that eliminates the need to redeploy the code to see those changes reflected in their app under development without restarting the application server.
JTA - Java Transaction API	JTA - Java Transaction API, enables distributed transactions to be done across multiple resources in a Java environment.
LDAP- Lightweight Directory Access Protocol	LDAP- Lightweight Directory Access Protocol, is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.

Table 4: Technical Tools	
Tool	**Definition**
Lightweight Enterprise Application Platform (LEAP)	HHSC Lightweight Enterprise Architecture Platform (LEAP) -see LEAP under modernization strategy section and TIERS Leap Architecture Reference document in the Procurement Library.
MVC - Model–view–controller	MVC - Model–view–controller, is a software architectural pattern for implementing user interfaces on computers. It divides a given software application into three interconnected parts, so as to separate internal representations of information from the ways that information is presented to or accepted from the user. Traditionally used for desktop graphical user interfaces (GUIs), this architecture has become extremely popular for designing web applications.
OpenJPA	OpenJPA, is an open source implementation of the Java Persistence JSR-317 Java Persistence 2.0 standard. It is an object-relational mapping (ORM) solution for the Java language, which simplifies storing objects in databases. It is an open source software distributed under the Apache 2.0 License.
POJO - Plain old Java object	POJO - Plain old Java object, is an ordinary Java object, not bound by any special restriction and not requiring any class path. The term "POJO" initially denoted a Java object which does not follow any of the major Java object models, conventions, or frameworks; nowadays "POJO" may be used as an acronym for "Plain Old *JavaScript* Object" as well, in which case the term denotes a JavaScript object of similar pedigree.
Qlik analytics engine	Qlik Analytics Platform is a suite that provides all the tools developers require to create unrestricted data-driven applications. Using visual analytics, and its modern analytics platform supports the creation and development of custom and guided analytics applications, including web mash-ups. The Qlik Analytics Platform can be used to apply business intelligence (BI) strategies to customers and partners via their extranet and internet sites. This helps to develop greater interaction and collaboration through data.
REST Web Service	REST - Representational State Transfer, is an architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. Through the application of REST architectural constraints certain architectural properties are induced: Performance, Scalability, Simplicity, Modifiability, Visibility, Portability, and Reliability.
SOAP	SOAP, originally an acronym for Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of web services in computer networks. It uses XML Information Set for its message format, and relies on application layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission

Table 4: Technical Tools	
Tool	**Definition**
Spring - Web MVC framework	Spring - Web MVC framework, provides model-view-controller architecture and ready components that can be used to develop flexible and loosely coupled web applications. The MVC pattern results in separating the different aspects of the application (input logic, business logic, and UI logic), while providing a loose coupling between the following elements: • The Model encapsulates the application data and in general they will consist of POJO. • The View is responsible for rendering the model data and in general it generates HTML output that the client's browser can interpret. • The Controller is responsible for processing user requests and building appropriate model and passes it to the view for rendering.
Websphere Application Server	A Java EE Standards based Web Application server.
Websphere MQ	Websphere MQ, is IBM's Messaging solution for Enterprise and IBM's Message Oriented Middleware offering. It allows independent and potentially non-concurrent applications on a distributed system to securely communicate with each other.
WS-Security - Web Services Security	Web Services Security, is an extension to SOAP to apply security to Web services. The protocol specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats.

Attachment C: TIERS Functional and Architecture Overview

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

Table of Contents

1. TIERS Applications and Business Functions 3

2. TIERS Business Processes 6

2.1 Telephone Call 6
2.2 Internet (Your Texas Benefits) 7
2.3 Fax and Mail 7
2.4 Community Based Organizations 7
2.5 HHSC Eligibility Office 7
2.6 TIERS Information Flows 9

3. Description of Operational / System Environment and Special Considerations 10

3.1 Operational Environment 11
3.2 System Information 11
3.3 Network Connectivity 13
3.4 Supporting Software Technologies 18
3.5 Databases and Data Stores 19
3.6 Functional Requirements 21
3.7 Architecture and Topology 26
3.8 System Boundary 29

4. Primary Platforms 33

4.1 TIERS Online 33
4.2 State Portal (STP) and Service Deliver Center (SDC) 33
4.3 Self Service Portal (SSP) - Your Texas Benefits (YTB) 33
4.4 Your Texas Benefits Mobile App (YTB Mobile) 33
4.5 DataMart 33
4.6 Enterprise Content Manager (ECM) 34
4.7 Enterprise Document Services (EDS) 34
4.8 Enterprise Web Services (EWS) 34
4.9 Document Center 34
4.10 Platform Components 34
4.11 Platform Components 38

5. E-Authentication Architecture, Products and Protocols 41

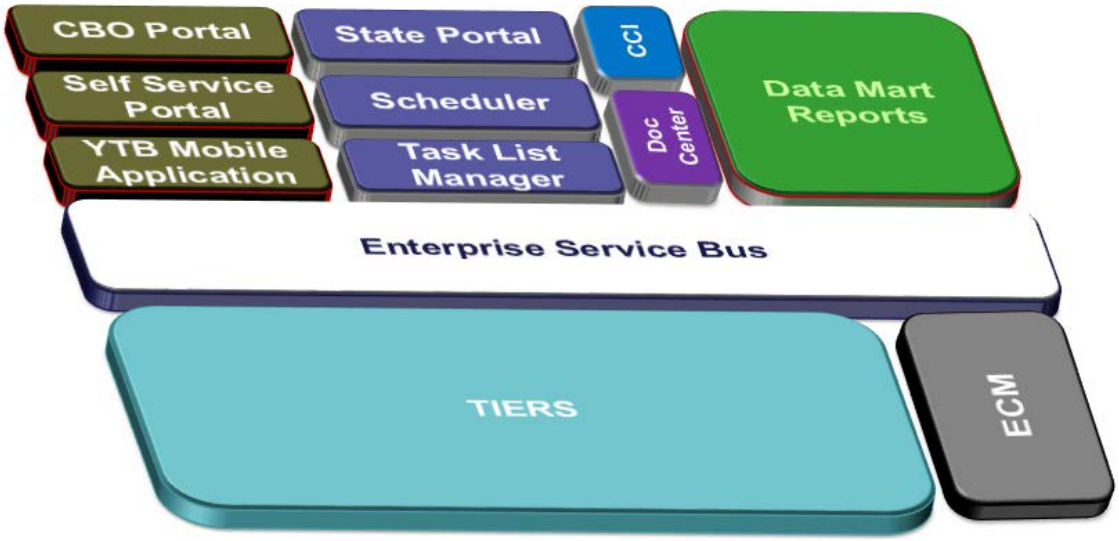
5.1 Description of Customer Groups Authenticated 42
5.2 Clerk 42
5.3 Supervisor 42
5.4 HHSC Eligibility CSR 43
5.5 Business Users 43
5.6 Client 43
5.7 Authorized Rep 43
5.8 CBO 44
5.9 Advisor 44

TIERS automates much of the rule-based processing to ensure consistency in eligibility determination. The integrated technologies and data sources also reduce the need for repetitive data-entry, photocopying and scanning tasks. TIERS brings several advantages to the state: improved customer service, expanded access to services without expanded paperwork, a more efficient platform for workers, enhanced fraud protection tools, and flexible technology that can adapt to changes in policy or law.

1. TIERS Applications and Business Functions

The primary applications of the TIERS system are depicted in Figure 1 - TIERS Applications Diagram, below.

Figure 1 - TIERS Applications Diagram



The names, acronyms and business functions associated with each of the applications are presented in Table 1 - Applications and Business Functions.

Table 1 - Applications and Business Functions

Name	Acronym	Business Function
Community Based Organizations Portal	CBO Portal	In an effort to make it easier and more efficient for Texans to apply for and manage their state benefits, HHSC is partnering with community-based organizations to assist people in learning about HHSC's benefits using the application and management website, YourTexasBenefits.com. Community Partner's organizations represent a wide range of social services, including public entities, non-profit organizations and faith-based groups. The CBO Portal is an enhanced version of the Self-Service Portal that provides additional functionality for CBO staff. This enhanced functionality is enabled based on CBO login to the SSP.
Your Texas Benefits (Self Service Portal)	YTB (SSP)	The YourTexasBenefits.com portal is available to clients 24 hours a day, 7 days a week. Applicants use this website to check the status of documents submitted to HHSC, submit applications, submit redeterminations, report changes, check the status of their benefits and check future appointments.
Your Texas Benefits Mobile Application	YTB Mobile App	A mobile application for people in Texas who have applied for or get SNAP food benefits, health-care benefits such as Medicaid and CHIP, or TANF. The mobile applications are available on iOS and Android platforms. The application supports many functions including: create a new account, upload supporting documents, view notices and reminders, submit change requests, locate nearby HHSC offices, check the status and amount of benefits and receive renewal notifications.

Name	Acronym	Business Function
State Portal / Service Delivery Center	STP / SDC	A single sign-on application where HHSC staff initiate tasks or work assignments, launch TIERS, view images and schedules, record complaints/requests for fair hearings and perform other activities related to eligibility determination.
Scheduler		A State Portal application that schedules and reschedules appointments for application, expedite or redetermination interviews.
Task List Manager	TLM	A State Portal application that manages tasks for HHSC staff. Staff select tasks based on workload availability or assignment. The TLM Global Queue and TLM Personal Queue are used to receive and monitor activities and due dates. The user role determines the tasks staff can view.
Call Center Inquiry	CCI	The Call Center Inquiry application assists customer service representatives in rapidly collecting TIERS information on a specific client or case. Development of a timeline to retire this application is under way.
Document Center	Doc Center	Document Center is an HHSC-owned application developed to support the vendor staff involved in pre-processing of documents received through channels: Mail, Fax, SSP, and Call Center. Pre-processing of documents includes but not limited to: classification, association to a TIERS case, and routing of a document to state staff for further processing
Data Mart Reports	DataMart	DataMart is a reporting system that pulls data from TIERS, TLM, STP and SSP. It then presents a set of operational reports to let TIERS users and management know the status of various activities in the system.

Name	Acronym	Business Function
Enterprise Service Bus	ESB	Enterprise Service Bus provides services and communication between applications in the middleware layer.
Texas Integrated Eligibility Redesign Systems	TIERS	The TIERS Core component (comprising TIERS Online, TIERS Batch, LUW Web Services, and TIERS database) includes a central data repository to collect eligibility information, a web interface, interfaces with other systems, decision table logic to process information and determine eligibility, and client notice generation.
Enterprise Content Manager	ECM	The Enterprise Content Manager provides the content and document management system for TIERS.

2. TIERS Business Processes

Access channels are the various ways TIERS clients can apply for benefits, check the status of submitted applications, report or check the status of a change, and several other options. Access channels include telephone, self-service, fax, mail, CBO, and in person at the Eligibility Offices.

2.1 Telephone Call

When a client calls 2-1-1 or 1-877-541-7905, a Customer Service Representative (CSR) provides information regarding State benefits and ways to apply for benefits. Services available by phone include:

Applying for benefits (excluding FS)

Screening for expedited food stamp eligibility

Checking the status of applications or benefits

Reporting changes

Requesting fair hearings

Rescheduling interviews

Responding to Missing Information letters

Checking the status of documents received by HHSC

Updating their phone number

2.2 Internet (Your Texas Benefits)

The Your Texas Benefits (YTB) Self Service Portal, online at www.yourtexasbenefits.com, is available to TIERS clients 24 hours a day, 7 days a week. They can use this website to check the status of documents submitted to HHSC, submit applications, submit redeterminations, report changes, check the status of their benefits, and check future appointments. Community based organizations and Qualified Entities / Qualified Hospitals also use Your Texas Benefits to enroll clients. The mobile application, Your Texas Benefits, is available on the iOS and Android platforms. The application supports many functions including: create a new account, upload supporting documents, view notices and reminders, submit change requests, locate nearby HHSC offices, check the status and amount of benefits, and receive renewal notifications.

2.3 Fax and Mail

Applications, changes and redeterminations received via fax and mail are processed according to the programs requested on the documents. Clients, authorized representatives, Community Based Organizations, and Eligibility Offices can fax and mail documents and applications directly to the TIERS document processing centers.

2.4 Community Based Organizations

HHSC is partnering with Community Based Organizations to help serve Texas communities. Level 1 CBOs provide clients with access to a computer and an internet connection to use the SSP to apply online for HHSC benefit programs. Level 2 CBOs also provide certified employees and volunteers to help people with using the SSP, submitting online applications, and managing their benefits online. Certified CBO employees and volunteers are called Your Texas Benefits navigators.

2.5 HHSC Eligibility Office

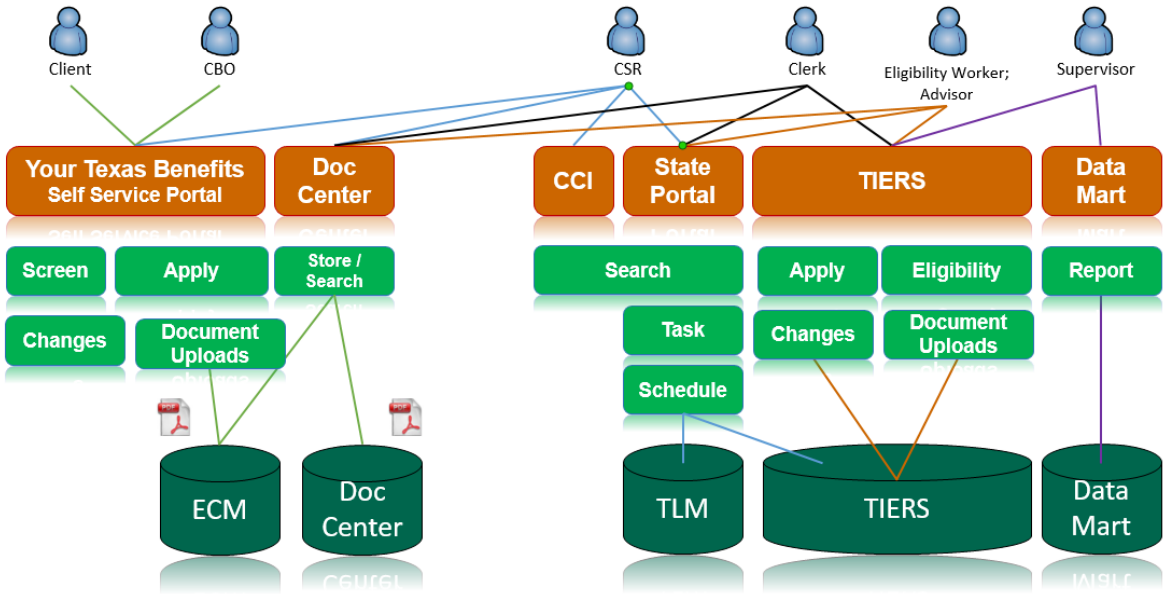
All documents received by the HHSC Eligibility Office are date stamped, reviewed for completeness and processed according to the guidelines for programs requested. They are routed to the document processing center when appropriate.

The underlying TIERS business processes are dependent upon the access channel used by the client and the type of action the client requires (e.g., apply for benefits, check the status of submitted applications, report a change, submit a redetermination, etc.).

Figure 2 - Overview of TIERS Business Processes provides an overview of the

TIERS business processes. Users are represented by the person icons at the top of the figure. The users interact with the TIERS system through different applications (shown under the users) depending on their user community, as shown by the connecting lines. The high-level processing functions supported by each application are represented in the ovals below each application. Finally, the data store supporting each process is represented at the bottom of the figure.

Figure 2 - Overview of TIERS Business Processes



Detailed HHSC business processes are defined by the following three documents:

Texas Works (TW) Handbook - includes policy and procedures for SNAP and other Texas Works programs. https://www.dads.state.tx.us/handbooks/texasworks/

MEPD Handbook - includes policy and procedures for Medicaid Eligibility for the Elderly and People with Disabilities (MEPD) program. https://www.dads.state.tx.us/handbooks/mepd/index.htm

State Processes - a manual that focuses on internal state processes and is designed to identify the core responsibilities of state eligibility determination staff (advisors, clerks, and management).

2.6 TIERS Information Flows

The information flows and interaction between the associated applications are described in the charts below. Federal Tax Information (FTI) is not stored, processed, or transmitted by TIERS.

Figure 3 - State Portal Architecture shows how data flows through the system as a result of user requests received from the State Portal (STP).

STP interfaces directly with the Self-Service Portal, Data Mart Reports, and TIERS core as necessary.

STP contains functionality from Scheduler, Task List Manager (TLM), Document Center, and Enterprise Content Manager (ECM).

Requests that involve the system data are sent to portal services and then coordinated by the middleware layer.

Figure 3 - State Portal Architecture

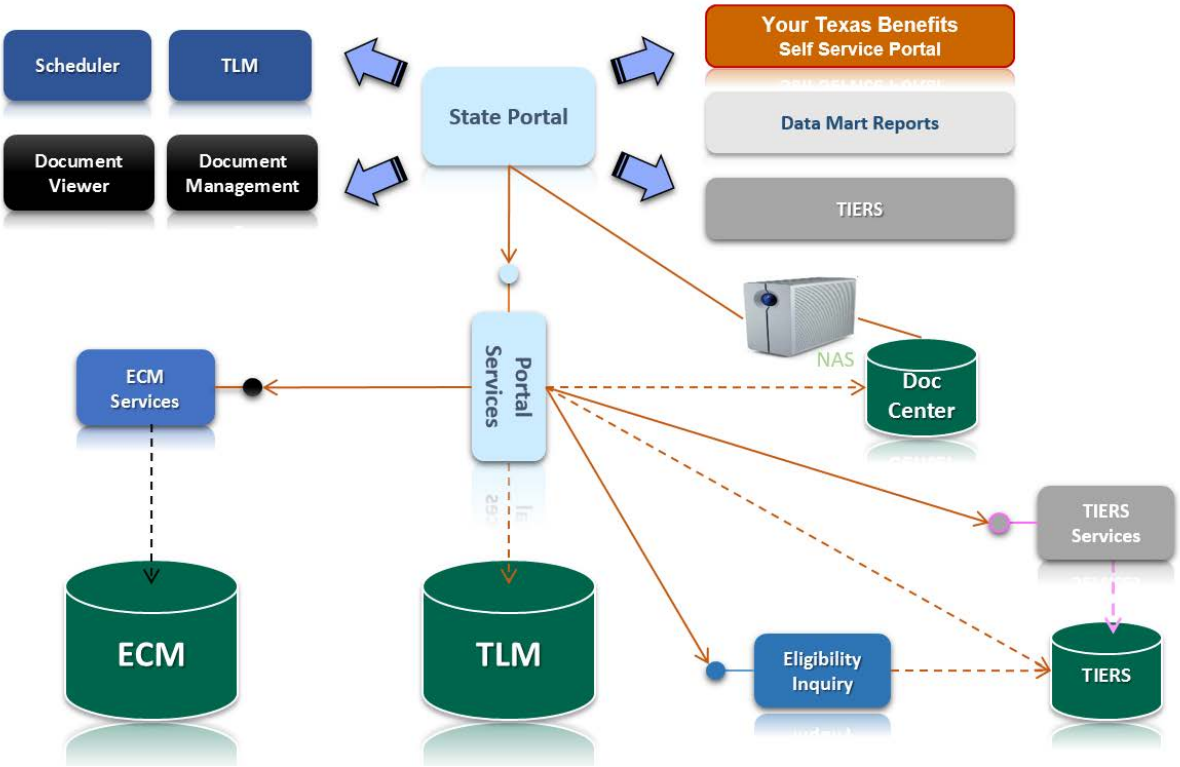
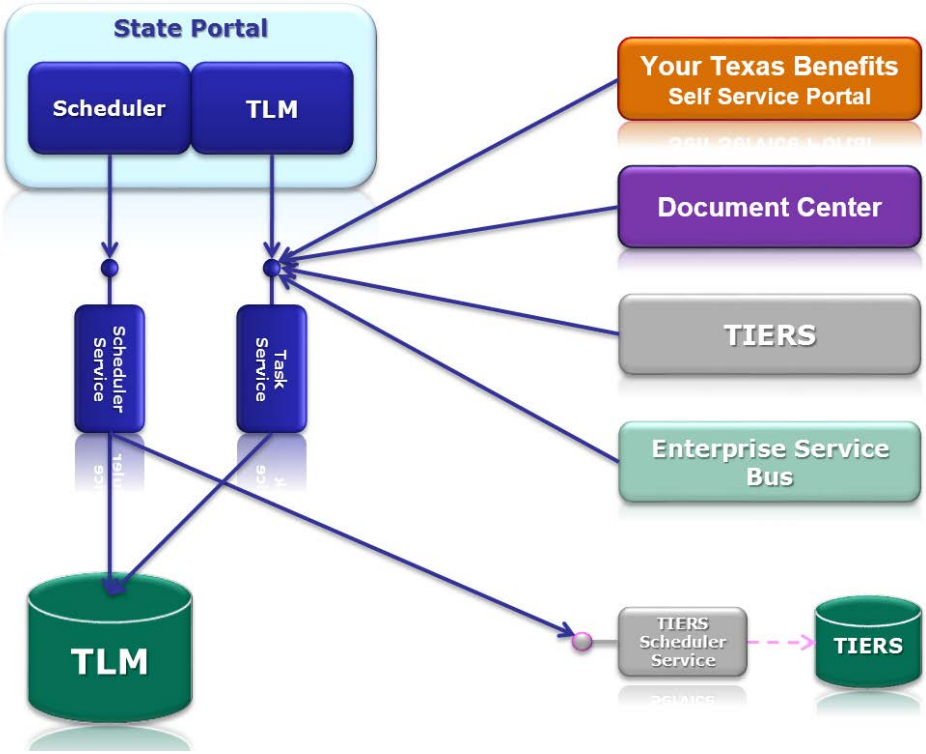


Figure 4 - Workflow Management Architecture shows how data flows into Task List Manager (TLM). Information is coordinated by the Task Service and the Scheduler Service and comes from:

Scheduler in the State Portal
Task List Manager
Self Service Portal / Your Texas Benefits
Document Center
TIERS
Enterprise Service Bus

Figure 4 - Workflow Management Architecture



3. Description of Operational / System Environment and Special Considerations

This section describes the system's operating environment, technical aspects, architecture, platforms, network connectivity, and additional security considerations.

3.1 Operational Environment

The TIERS operating environment consists of:

Data Centers (Winters and San Angelo)

a. The data centers contain the IT infrastructure that supports the operation of the TIERS system. Winters is the primary data center for production and development activities. San Angelo is a disaster recovery (DR) data center; all data from Winters is replicated to San Angelo. The data centers are operated by a vendor.

Call Centers

a. The call centers provide incoming phone support for clients and interact with the information system on their behalf. The call centers are operated by a vendor.

Public Offices

a. Public benefits offices are located throughout the state of Texas and staffed by state employees. These offices support face-to-face interaction with clients.

Document Processing Facilities

a. The document processing facilities are responsible for receiving client documents via mail/fax, storing those documents in Document Center, and submitting that information to the system.

3.2 System Information

The TIERS technical system consists of a collection of information systems spanning multiple platforms. With 28 environments, 3100+ Virtual Systems and over 390 servers, the TIERS system supports over 10,000 unique users a day. A redundant network designed to support a high volume of data has been implemented, along with complementary security components designed to protect the data. All network devices have redundant components for enhanced availability. This infrastructure supports the set of applications listed in Table 1, which enable the TIERS system to meet its business needs.

A high-level snapshot of the system infrastructure is presented below:

Database on Oracle supercluster with a production database size over 50 TB (multiple Standbys/Repos). Over 1 PB allocated to support databases for all dev, test, training and DR environments.

Content management systems storing over 190 million inbound documents and growing at about 1.3 million per month. 62 TB of storage for all correspondence is also managed and maintained.

The TIERS application runs on 379 physical servers including Linux, Solaris and Windows operating systems supporting over 3200+ virtual systems.

Middleware tier includes technologies like IBM WebSphere, Adobe Enterprise Manager, Cognos, Informatica to support portals, content generations (forms, PDFs), and reports.

Applications are mostly Java J2EE based modules that interact with browser based or portal-based user interfaces through web services.

a. TIERS core applications support over 5 million eligibility determination transactions per day with a workload of 100,000 tasks per day.

b. Online web portals provided to all Texas residents take in over 10,000 new applications and about 10,000 change and redetermination of benefits applications. These are processed with set timeliness standards. In addition, over 50,000 paper applications are submitted daily via mail, fax and phone channels.

c. Workloads for eligibility staff includes about 12,000 walk-in/phone appointments and a completion of about 100,000 tasks, done in benefit offices across the state.

d. Interfaces including SOAP/rest services (hardened), point to point tunnels and SFTP sites to over 30 partners. These interfaces are used for data exchange on a daily, weekly, monthly basis.

e. Over 100 web services (SOAP, REST) help with the orchestration between the various applications and components. These are supported with IBM WebSphere based appliances like DataPower, Business Process Manager (BPM) and Operational Decision Manager (ODM).

Interfaces including SOAP/rest services (hardened), point to point tunnels and SFTP sites to over 30 partners.

a. Web services (hardened through DataPower) – 35 services

b. MQ (point to point tunnel) – 7 Queues

c. SFTP (unique files – same file sent to multiple Trading Partner):

	Receive Files	Send Files
Daily	64	160
Weekly	12	10
Monthly	36	150
Quarterly	5	7
Annual	10	12

Over 100 web services (SOAP, REST) help with the orchestration between the various applications and components. These are supported with IBM WebSphere based appliances like DataPower, Business Process Manager (BPM) and Operational Decision Manager (ODM).

Deployment tools like Jenkins and CI/CD process to enable monthly releases to production are supported in-house. IBM ClearCase is used as the software configuration management of source code, configuration and other software development assets. These are maintained on-premise. The TIERS Configuration Management Plan is included as Attachment D.

Identity management for TIERS applications is governed by HHSC and uses IBM suite of products like Security Access Manager (ISAM), Privileged Identity Management (PIM). Data integrity and security is also maintained using encryption at rest and in transit.

Networks to support TIERS applications are maintained and managed by HHSC IT vendors. Network security includes Layer 3 and Layer 7 firewalls, WAF using F5 and/or CISCO appliances.

Tools to support 24x7 monitoring and gathering operational metrics

3.3 Network Connectivity

Figure 5 - Network Connectivity Diagram depicts the TIERS network connectivity diagram. The network components in this diagram are numbered. The chart below provides a reference for this network diagram to show the component's name along with its function. Note that critical network components that pass TIERS traffic have redundant links (routers, firewalls, switches).

Figure 5 - Network Connectivity Diagram

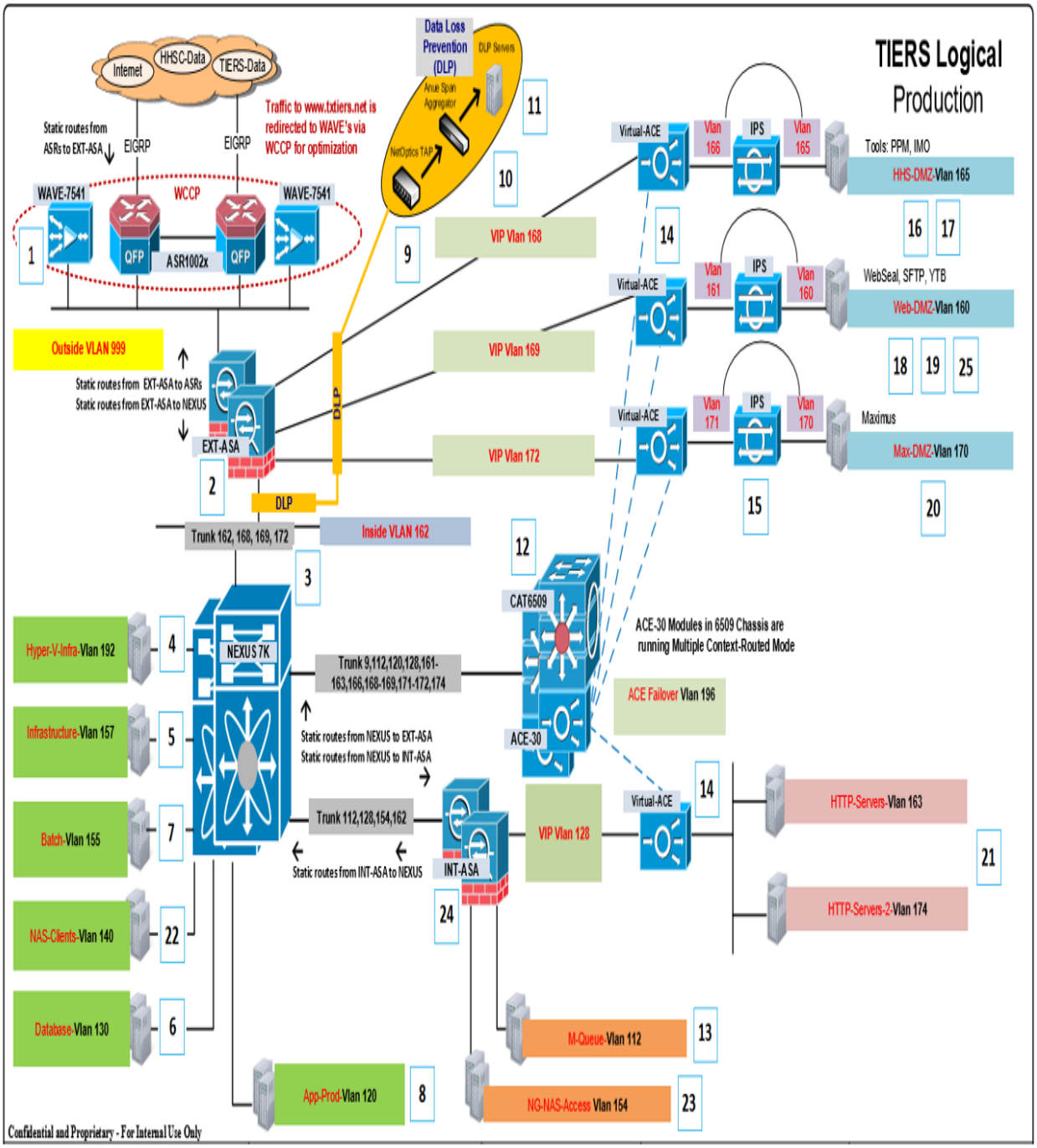


Table 2 - Network Component Breakdown

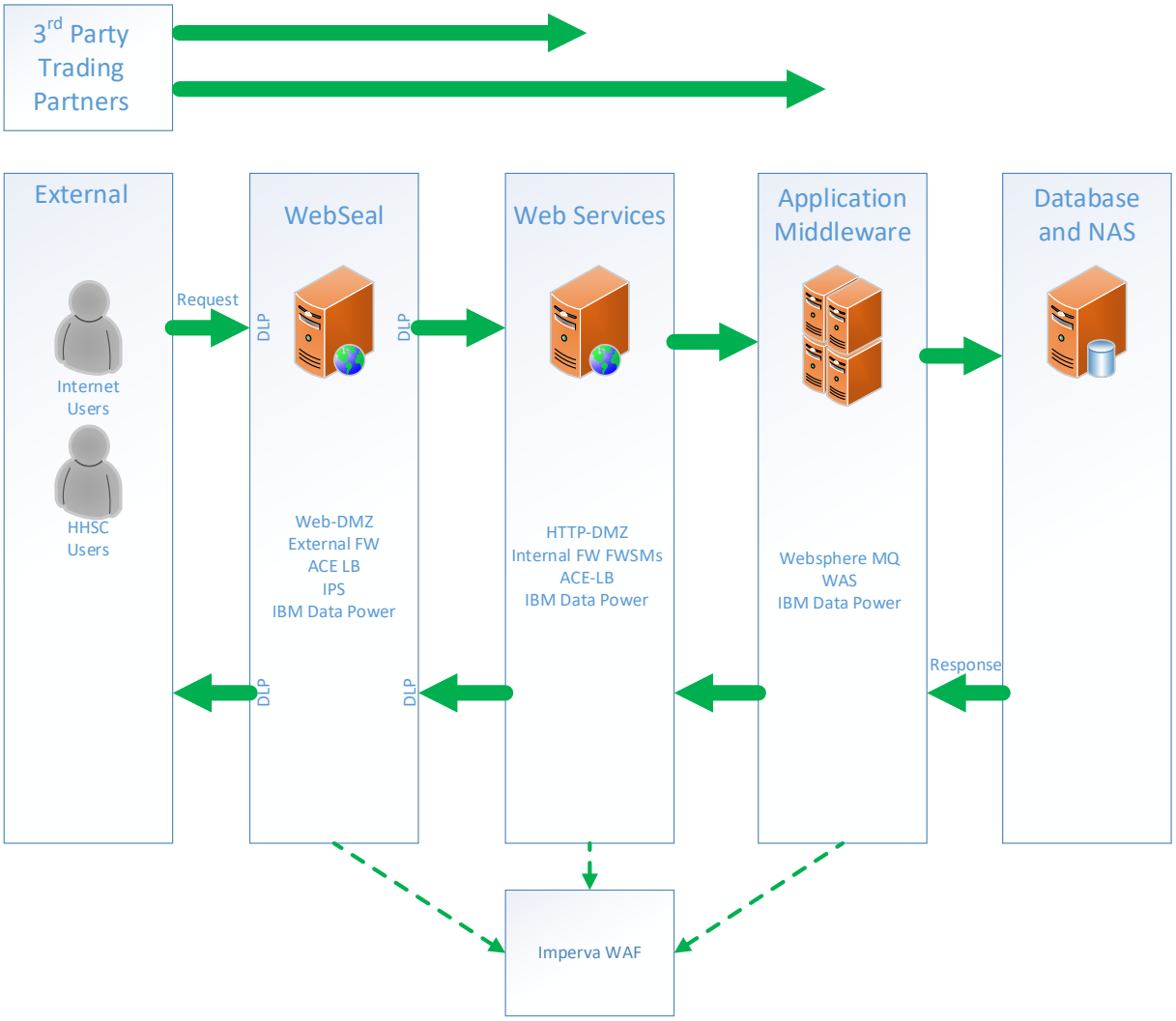
Network Component Number	Network Component Name	Function
1	Cisco ASR 1002 (Border Routers)	Connects the TIERS network with the public-untrusted internet
2	Cisco EXT-ASA FW (Border Firewalls)	Provides advanced security between three networks (trusted, untrusted, and the DMZ).; Provides additional security (deep packet inspection, firewall, ACLs); compatible with 5G or 10G configurations. The DMZ is between these firewalls.
3	Layer 3 Nexus Switch	Provides layer 2 functionality (VLANs) along with layer 3 routing protocols; Allows devices to talk to other VLANs and/or networks
4	Hyper-V Server VLAN 192	Used for x86 and x64 OS virtualization
5	VLAN 157 File Server (Infrastructure)	Supports SSH, SFTP, SCP, NTP, NAS
6	VLAN 130 Database	Multiple databases with data that is stored and retrieved by applications
7	VLAN 155 Batch Process Servers	Perform batch jobs
8	VLAN 120 App Production Server	Servers that handle the production processing for TIERS
9	Net Optics TAP	Allows access for in-line security and network monitoring devices
10	Anue Span Aggregator	Aggregates traffic to assist monitoring
11	DLP Servers	Home for DLP software and tools; designed to prevent users from sending sensitive or critical information outside of a corporate network; also helps admins control

Network Component Number	Network Component Name	Function
		which types of data end users are allowed to transfer over a network
12	Layer 2 Service Chassis	Layer 3 switch performing layer 2 and layer 4 functionality.
13	VLAN 112 M-Queue Server	Provides channels for communications between applications or between application and server; allows asynchronous communication
14	Load Balancers	Maximizes resources by distributing workload across multiple servers. It minimizes response time, maximizes throughput, avoids overload, and is responsible for SSL terminations.
15	IPS	Intrusion Prevention System: designed to actively monitor and prevent malicious software/intrusions on the network, and sends alerts to admins
16	VLAN 165 Project and Portfolio Management (PPM)	Suite used for Change Management
17	VLAN 165 Infrastructure, Maintenance, & Operations (IMO)	Applications to support TIERS infrastructure, maintenance, and operations
18	VLAN 160 WebSeal	A high performance, multi-threaded Web server that is designed to apply fine-grained security policies to the Tivoli Access Manager protected Web object space.

Network Component Number	Network Component Name	Function
19	VLAN 160 sFTP	Server that is used for approximately 80% of transferred files to/from trading partners
20	VLAN 170 MAXIMUS (Call Center Vendor)	Servers to support information exchange with MAXIMUS (Call Center vendor)
21	VLAN 163 and 174 HTTP Servers	Used to host publicly accessible web pages
22	VLAN 140 NAS Clients	Network attached storage to support MAXIMUS operations
23	VLAN 154 NG NAS Access	Provides administrative access to VLAN 140 for operations and maintenance
24	Cisco INT-ASA FW (Firewalls)	Firewall between the HTTP servers and the internal network
25	VLAN 160 Your Texas Benefits (YTB)	Applications and services to support the Your Texas Benefits mobile and web applications

Figure 6 - Network Request Path shows how the network is layered with security zones to handle network requests from users. All user requests are authenticated by and terminated at WebSeal. WebSeal then communicates with web services, which makes a call on the application middleware, which then handles communication with the database. User requests cannot bypass WebSeal. The only conditions where WebSeal may be bypassed is by trusted third-party trading partners who may access web services and/or middleware without first authenticating with WebSeal. The response to a request is passed back through the layers it traveled down in reverse order, going through each zone of security to get to the next layer. Data passing through WebSeal is covered by Data Loss Prevention (DLP).

Figure 6 - Network Request Path

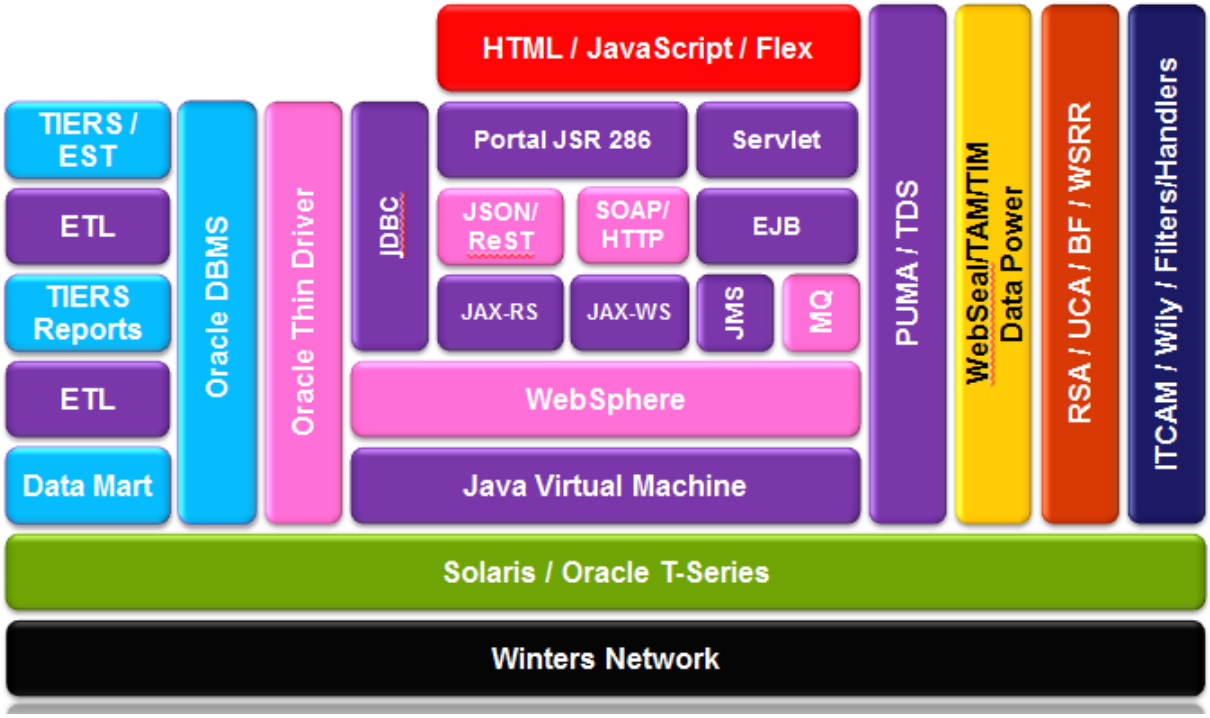


In addition to the security measures shown above, there are software tools that cover monitoring and vulnerability management such as Symantec CCS and additional tools shown in the TIERS Information System Architecture diagram.

3.4 Supporting Software Technologies

Figure 7 - TIERS Supporting Software Technologies shows the supporting software technologies that underlie TIERS. The bottom of the figure shows that the software runs in the Solaris environment in the Winters Data Center. The supporting software technologies are shown in the middle. On the left are the applications they support and, on the right,, their internal interfaces. Dataflow through TIERS internally is managed and coordinated by the WebSphere MQ solution in response to user requests.

Figure 7 - TIERS Supporting Software Technologies



3.5 Databases and Data Stores

Table 3 lists the databases and data stores used by TIERS.

Table 3 - TIERS Database List

Database Type	Data Base Name	Backend For
Oracle (Of over 300 Oracle databases in the TIERS system, only the production databases are listed here for brevity)	Database 1	Build Forge
	Database 1	COTS
	Database 2	ECM
	Database 3	Chip
	Database 4	ECM
	Database 5	Cognos
	Database 6	DBA Logical
	Database 7	Datamart
	Database 8	Datamart
	Database 9	QC/PerfCenter
	Database 10	I3
	Database 11	Informatica

Database Type	Data Base Name	Backend For
	Database 12	PPM
	Database 13	COTS
	Database 14	MQ
	Database 15	Perinatal
	Database 16	DBA Physical
	Database 17	Process Server
	Database 18	Tiers
	Database 19	Qpasa
	Database 20	Qpasa
	Database 21	Rational
	Database 22	Tiers
	Database 23	DBA Physical
	Database 24	COTS
	Database 25	COTS
	Database 26	COTS
	Database 27	Serena
	Database 28	TLM
	Database 29	Tiers
	Database 30	Tiers
	Database 31	State Portal
	Database 32	TLM
	Database 33	STP LDAP - State Portal
	Database 34	SSP LDAP - Self Service Portal
DB2	Database 35	TIM LDAP - Tivoli Identity Manager
	Database 36	TIM LDAP - Tivoli Identity Manager
	Database 37	Opcon - No Cluster
	Database 38	Opcon - No Cluster
SQL	Database 39	Moxie Prod
	Database 40	Moxie Dev
	Database 41	KOFAX Prod, Node 1 WDC SQL cluster,

Database Type	Data Base Name	Backend For
		located at the Austin WDC, supports all Kofax Fax Channel processing functions
	Database 42	KOFAX Prod, Node 2 WDC SQL cluster
	Database 43	KOFAX Prod, Node 1 DPC SQL cluster, located at the Austin Kramer DPC, supports all Kofax Mail Channel scanning functions
	Database 44	KOFAX Prod, Node 2 WDC SQL cluster
	Database 45	KOFAX Test Located at the Austin Kramer DPC
	Database 46	KOFAX Test Located at Austin WDC
	Database 47	KOFAX Dev Located at Austin WDC
	Database 48	KOFAX DR Located at Athens Kofax DR site
	Database 49	IMO SharePoint

3.6 Functional Requirements

The purpose of the TIERS information system is to provide a smooth and integrated process for clients to determine their eligibility for the government assistance programs. The TIERS information system is capable of:

Receiving applications by office visit, phone, mail, fax, online, or through partners.

Collecting the required information and determining eligibility based on a set of eligibility rules.

Providing an eligibility decision within the required amount of time.

Handling over 7 million transactions a day.

Table 4 - TIERS Functional Requirements documents the functional requirements of the system.

Table 4 - TIERS Functional Requirements

TIERS Functional Requirements
Firewalls are required in to secure the TIERS system. These firewalls must contain the following: a. Access Control Lists (ACL) b. Virtual Private Networks (IPSec, L2TP) c. Intrusion Prevention Systems (IPS) d. Web Application Firewalls (WAF) e. Symantec (Anti-virus and security tool suite) **f.** Support Secure Protocols (SSL, SSH, SFTP, HTTPS)
A web server infrastructure is required.
An internal email system is required. This system and its infrastructure are not maintained by TIERS.
A mechanism for employees to access the internal network via VPN is required to support telecommuting.
The system must support the Solaris operating system.
The system is required to have the necessary NAS, SAN, server, and networking hardware to support the applications.
The system must have high network availability to meet end user needs.
The system must support virtualization.
The system is required to be secured on all levels: application, presentation, session, transport, network, data link, and physical.
The system must support data transmission, storage/archival, and processing & reporting of information.
The system must implement a disaster recovery and business continuity plan.
The system must have test and dev environments to support development and deployment of improvements.
The system must include environments for load and stress testing.

TIERS Functional Requirements
The system must include an interface with postal mail.
The system must be able to accept incoming applications by office, mail, fax, phone, online, and from partners.

Table 5 - Systems Users shows the user types, organizations (internal and external) comprising the user community, levels of access, Uniform Resource Locator (URL) for web-based access, and how the system is accessed

Table 5 - Systems Users

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)
Clients	External	Read/write access to their application and case information.	Application and case information	TCP/IP, HTTPS	https://www.yourtexasbenefits.com
Community Based Organization (CBO)	External	Limited search for some roles. Read/write access to application and case information for client logged in	Application and case information for client logged in	TCP/IP, HTTPS	https://www.yourtexasbenefits.com
Qualified Hospital /	External	Limited search for	Case information		

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)
Qualified Entity (QH / QE)		some roles. Read/write access to application and case information for client	for Presumptive Eligibility Determinations.	TCP/IP, HTTPS	https://www.yourtexasbenefits.com
Customer Service Representative (CSR)	Internal	Read/write access to application and case information	Application and case information	TCP/IP, Web Portal via Desktop Terminal Services	https://www.txtiers.net/cciApp/CallCenterInquiry/HTML/CCISearch.jsp
HHSC Clerk	Internal	Read/write access to application and case information	Application and case information	TCP/IP, HTTPS	https://www.txtiers.net
HHSC Eligibility Worker	Internal	Read/write access to application and case information	Application and case information	TCP/IP, HTTPS	https://www.txtiers.net
HHSC Supervisor	Internal	Read/write access to application and case information	Application and case information	TCP/IP, HTTPS	https://www.txtiers.net

User Type (Group or Role)	Internal / External	Access Rights (Read, Write, Modify, Delete	Data Type Accessed	User Interface (How system accessed – TCP/IP, Dial, SNA, etc.)	Web-Based Access (Provide URL)
TIERS Developer /Tester	Internal	Read/write access to application and case information in testing environments	Application and case information in testing environments	TCP/IP, HTTPS	
Infrastructure Application Support (DBA)	Internal	Read/write access; Database Administration (Privileged Access).	Databases	TCP/IP	
Infrastructure Application Support (Middleware)	Internal	Read access	Middleware	TCP/IP	
Data Center Operations	Internal	OS access only (read/write)	Operating Systems	TCP/IP, SSH	

3.7 Architecture and Topology

The architecture of the TIERS information system can be broken down into three layers: the presentation layer, the application layer, and the data layer, as shown in Table 6 - Architectural Security Considerations.

Table 6 - Architectural Security Considerations

Architectural Layer	Components	Security Reasoning
Presentation Layer	Security & Presentation Identity Management	All user functions are conveniently made available to the users via web interfaces, users cannot access internal resources directly
Application Layer	Middleware Messaging Services Monitoring & Vulnerability Management Business Intelligence Infrastructure Batch Trading Partner Interfaces	All user requests are handled by applications that operate securely within the TIERS network
Data Layer	Production Data Training Data Meta Data DB	Access to the TIERS databases is given to internal applications and is controlled by WebSphere MQ

The system architecture is further detailed in Figure 7 - TIERS Information System Architecture, and the architectural groupings from this figure correlate to the components documented for the presentation, application, and data layers shown in Table 6 - Architectural Security Considerations, above.

Figure 7 - TIERS Information System Architecture

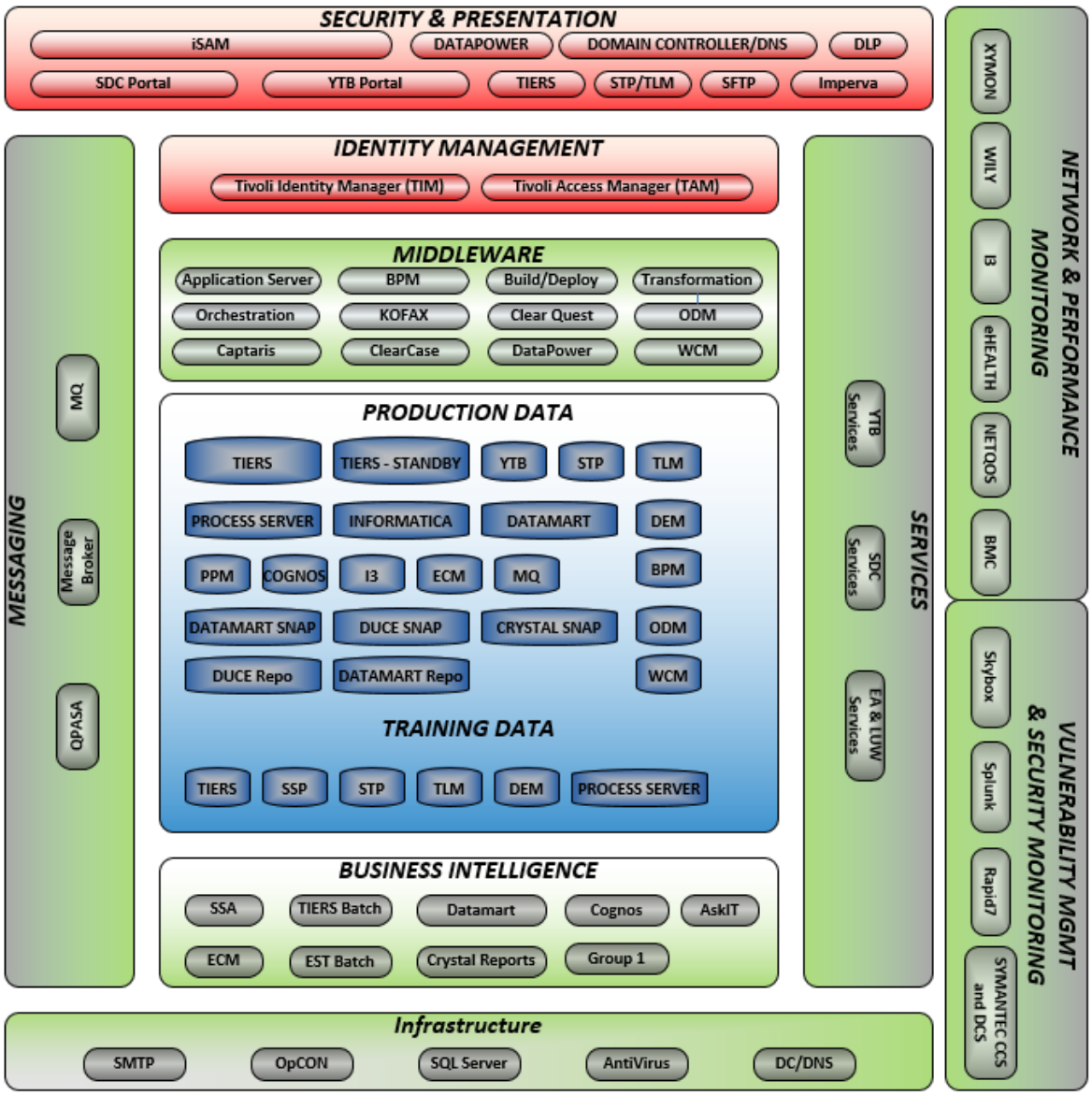


Figure 8 - TIERS Functional Architecture shows the functional architecture of the system. The users and trading partners are represented by the person icon. The users interact with the system through different interfaces depending on their role, as shown by the connecting lines. All users interact with the system using the presentation layer (shown in red), except for the trusted trading partners whose connections are carefully established through interfaces or Data Power/ESB. The middleware/applications (shown in green) respond to user requests and interfaces with the databases (shown in blue) as necessary. Figure 9 - Infrastructure Topology of TIERS shows the infrastructure topology of the system.

Figure 8 - TIERS Functional Architecture

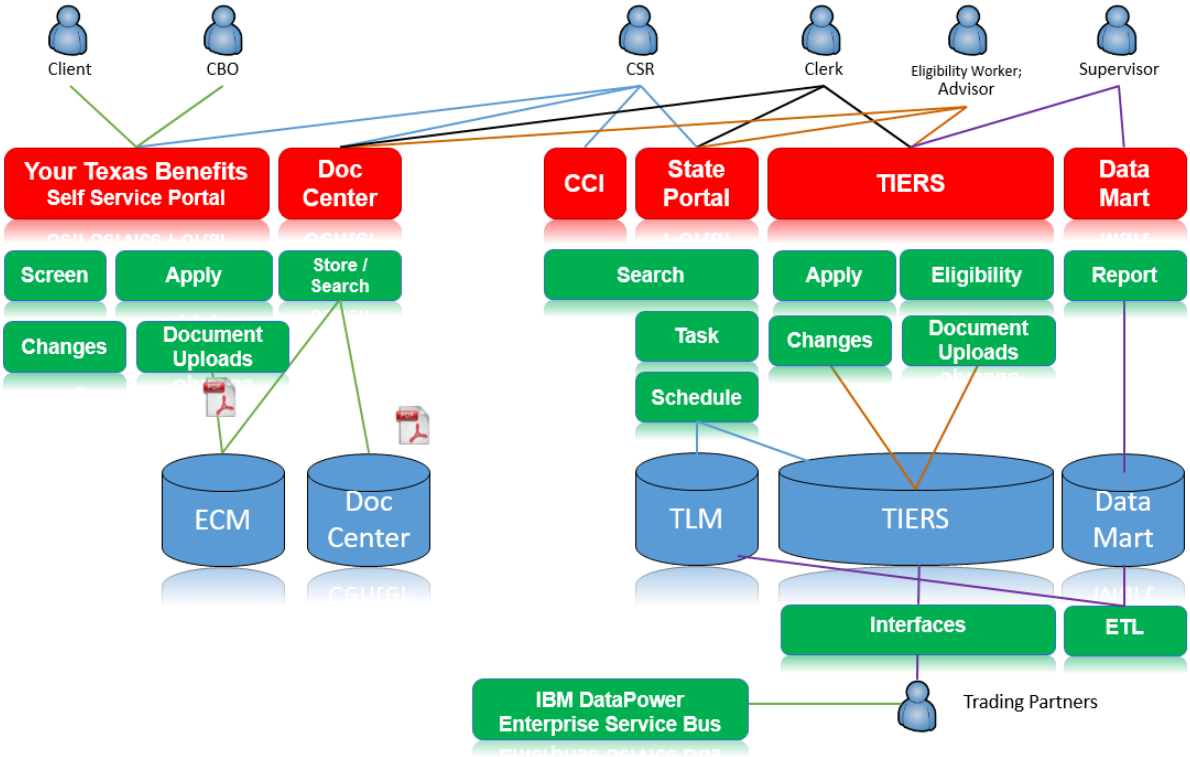
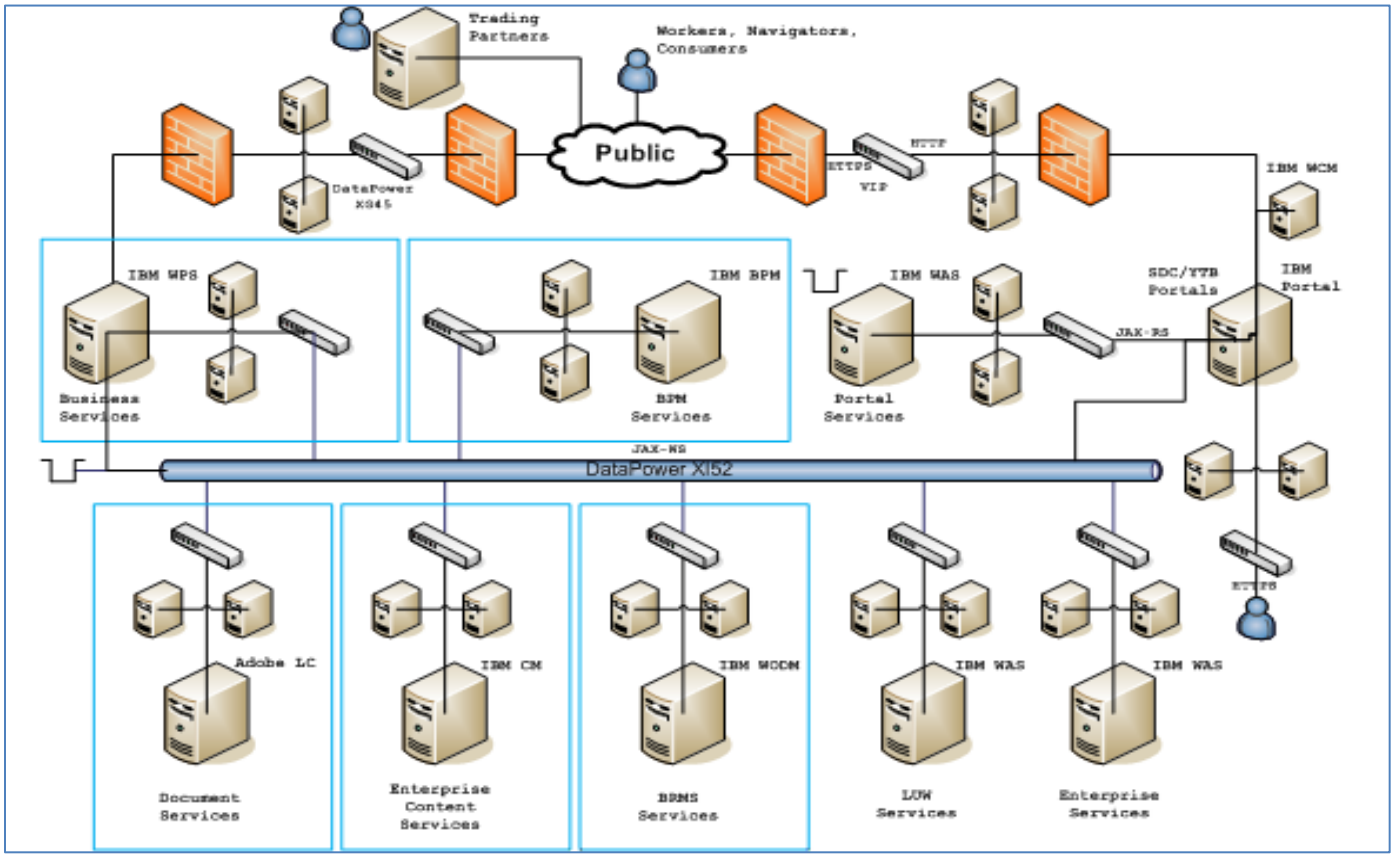


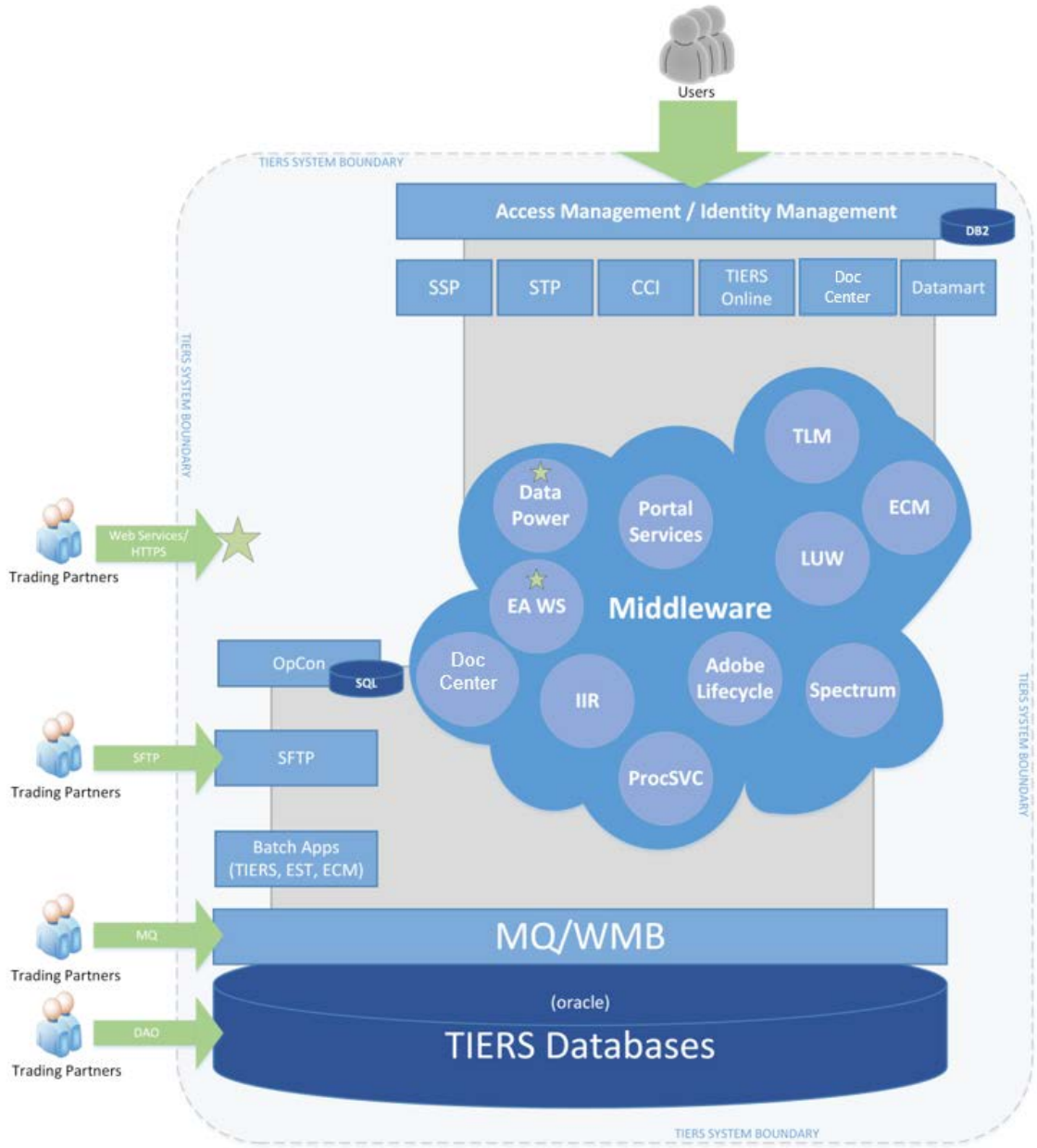
Figure 9 - Infrastructure Topology of TIERS



3.8 System Boundary

The TIERS information system boundary contains the components of the system whose primary purpose is to support the operation of TIERS. The parts of the system that are outside of the boundary include users and trading partners. The system boundary is depicted in Figure 10 - TIERS System Boundary, which shows what is inside the boundary, what is outside the boundary, where they connect, and how they connect.

Figure 8 - TIERS System Boundary



Information flows into the system from users and trading partners, then that information is stored in the TIERS database. The flow of that data through the system varies depending on specific requests from users/applications, and is coordinated by the WebSphere MQ component.

Table 7 - TIERS Externally Connected Parts lists the parts of the TIERS information system that communicate over the boundary.

Table 7 - TIERS Externally Connected Parts

Part	Category	Access Information
Identity Management	Software	All users accessing the system must authenticate with Tivoli identity/access management first
SSP / YTB Portal	Software	After users are authenticated they can access the user interfaces in SSP based on their role. New SSP users are required to go through two factor identification and authentication during account setup. The users verified via two-factor authentication are granted case visibility access and can see case data and submit changes. Unverified users are given application visibility access to apply for benefits and view prior applications submitted via their SSP user names.
STP / SDC Portal	Software	After users are authenticated they can access the user interfaces in STP based on their role
TIERS Online	Software	Authenticated users with appropriate permissions can access the TIERS Online user interface.
Document Center	Software	Authenticated users with appropriate permissions can access the Document Center user interface.
DataMart	Software	Authenticated users with appropriate permissions can access the DataMart user interface. DataMart is an IBM Cognos product.
Your Texas Benefits mobile app	Software	Mobile application that allows authenticated users access to SSP interfaces based on their roles.
DataPower	Hardware	The IBM DataPower device communicates with trading partners via web services
EA Web Services	Software	The Enterprise Application Web Services application communicates with trading partners via web services
CCI	Software	The Call Center Inquiry interface is designed for call center reps to interact with the system on the client's behalf while on the phone with them

Part	Category	Access Information
sFTP	Software	A majority of the information intake for the TIERS system occurs by trading partners depositing data via sFTP
MQ / WMB	Software/ System Interface	The WebSphere MQ application coordinates data transfer with trading partners
TIERS Database	Software/ System Interface	A small number of trading partners make data access object (DAO) calls directly on the database over VPN through established interfaces

4. Primary Platforms

The primary platforms of the TIERS system are:

4.1 TIERS Online

TIERS Online serves as a case management system used by HHSC staff for determining TIERS applicant's eligibility. TIERS Online was built off of Java EE 7 and uses a custom Java framework. This system contains over 7.3 million lines of code, utilizes 10,112 business rules, pulls data from 1,998 database tables, and handles over ten million users daily.

4.2 State Portal (STP) and Service Deliver Center (SDC)

State Portal was designed to be used for administration and task management and is used by both HHSC staff as well as vendor staff. It uses Java JSR 286 portlets and Java EE 7. Additionally, the STP component utilizes the Struts framework, Springs framework, JavaServer Faces (JSR), Ajax, Dojo toolkit, Hibernate, Java Persistence API (JPA), and contains approximately three million lines of code.

4.3 Self Service Portal (SSP) - Your Texas Benefits (YTB)

The Your Texas Benefits Portal was designed to enable clients (end users) to directly interface with the TIERS system. This web application helps to screen and determine applicant eligibility. The YTB portal includes the Self-Service Portal (SSP) and Long Term Services and Supports (LTSS). Community based organizations and Qualified Entities / Qualified Hospitals also use the Self-Service Portal in addition to customers. The SSP is based off of the Adobe Flex framework, Adobe LiveCycle Data Services (LCDS), and Java SE 7. It utilizes a custom-built Java Persistence API and has approximately one million lines of code. This component of the system handles approximately 64,600 users per day.

4.4 Your Texas Benefits Mobile App (YTB Mobile)

The mobile application, Your Texas Benefits, is available on the iOS and Android platforms. The application supports many functions including: create a new account, upload supporting documents, view notices and reminders, submit change requests, locate nearby HHSC offices, check the status and amount of benefits, and receive renewal notifications.

4.5 DataMart

DataMart is a reporting system that pulls data from TIERS, Workforce Management, STP and SSP. It then presents that data from these systems

as a set of operational reports to let TIERS users and management know the status of various activities in the system. DataMart contains large amounts of Personally Identifiable Information (PII). DataMart access is authenticated by the identity management system (IBM Tivoli Identity Manager / Tivoli Access Manager), and the State Portal. Also, DataMart imports data from LDAP to determine which organization a worker belongs to. This enables TIERS to restrict a user's access to data based on organization. The system was built off of Informatica ETL (Extract, Transform and Load) and IBM Cognos and contains less than one million lines of code.

4.6 Enterprise Content Manager (ECM)

Enterprise Content Manager was designed as a document management system for HHSC and vendor staff. It is based off of the Java EE 7 platform, utilizes a custom framework, and contains less than one million lines of code. ECM serves as an image repository.

4.7 Enterprise Document Services (EDS)

EDS was implemented as a PDF generating engine for producing and merging documents, and primarily provides this service to other applications in the middleware layer. It is based off of Adobe LiveCycle and contains less than one million lines of code.

4.8 Enterprise Web Services (EWS)

Enterprise Web Services provides services and communication between applications in the middleware layer. EWS uses Business Process Execution Language (BPEL) as its executable language.

4.9 Document Center

Document Center is a HHSC owned application developed to support the vendor staff involved in pre-processing of documents received through channels: Mail, Fax, SSP, and Call Center. Pre-processing of documents includes but not limited to: classification, association to a TIERS case, and routing of a document to state staff for further processing

4.10 Platform Components

The components and associated security concerns for each of the platforms are summarized in Table 8.

Table 8 - TIERS Platforms and Components

Platform	Components	Category	Security Concerns and Implemented Controls
TIERS Online	Number of Servers: 33 VLANs:160, 163, 120, 121, 130	Hardware	Firewalls in place to mitigate threats from public internet; Data center has strong physical security and access controls to prevent unauthorized access.
	Oracle 11g Java Enterprise Edition 7	Software	Applications require authentication from WebSeal to communicate with TIERS. Known vulnerabilities: XSS, Injection, and malicious code execution. Countermeasures: input validation, strong output encoding, uses strongly typed parameterized query APIs.
State Portal (STP) and Service Delivery Center (SDC)	Number of Servers: 31 VLANs:160, 163, 120, 121, 130	Hardware	Firewalls are in place to mitigate threats from public internet; Data center has strong physical security and access controls to prevent unauthorized access.
	Java Enterprise Edition 7 Struts JSF AJAX Dojo Spring Hibernate JPA Adobe Flex IBM Portal IBM WebSphere	Software	Applications require authentication from WebSeal to communicate with TIERS. Known vulnerabilities: XSS, Injection, and malicious code execution. Countermeasures: input validation, strong output encoding, uses strongly typed parameterized query APIs.

Platform	Components	Category	Security Concerns and Implemented Controls
Self-Service Portal (SSP) - Your Texas Benefits (YTB); YTB Mobile	Number of Servers: 36 SSP: 33 LiveCycle: 3 VLANs:160, 163, 120, 121, 130	Hardware	Firewalls are in place to mitigate threats from public internet; Data center has strong physical security and access controls to prevent unauthorized access.
	Adobe Flex framework Adobe LiveCycle Data Services (LCDS) Java Enterprise Edition 7 Java SE Java Persistence API Appcelerator Titanium (for IOS and Android mobile apps)	Software	Applications require authentication from WebSeal to communicate with TIERS. Known vulnerabilities: XSS, Injection, and malicious code execution. Countermeasures: input validation, strong output encoding, uses strongly typed parameterized query APIs.
DataMart	Number of Servers: 10 Informatica: 2 Cognos: 8 VLANs:120	Hardware (ver.28 doc)	Firewalls are in place to mitigate threats from outside world; Data center has strong physical security and access controls to prevent unauthorized access. Connections are only permitted inside the HHSC network.
	Informatica ETL IBM Cognos Oracle	Software (ver.28 doc) (include app software and OS Software)	Reporting Tools, IIR, Powercenter, PPM, and Quality Center may contain a lot of PII/PHI. These tools require a secure connection and authentication by IBM Tivoli Identity Manager / Tivoli Access Manager (TIM/TAM).

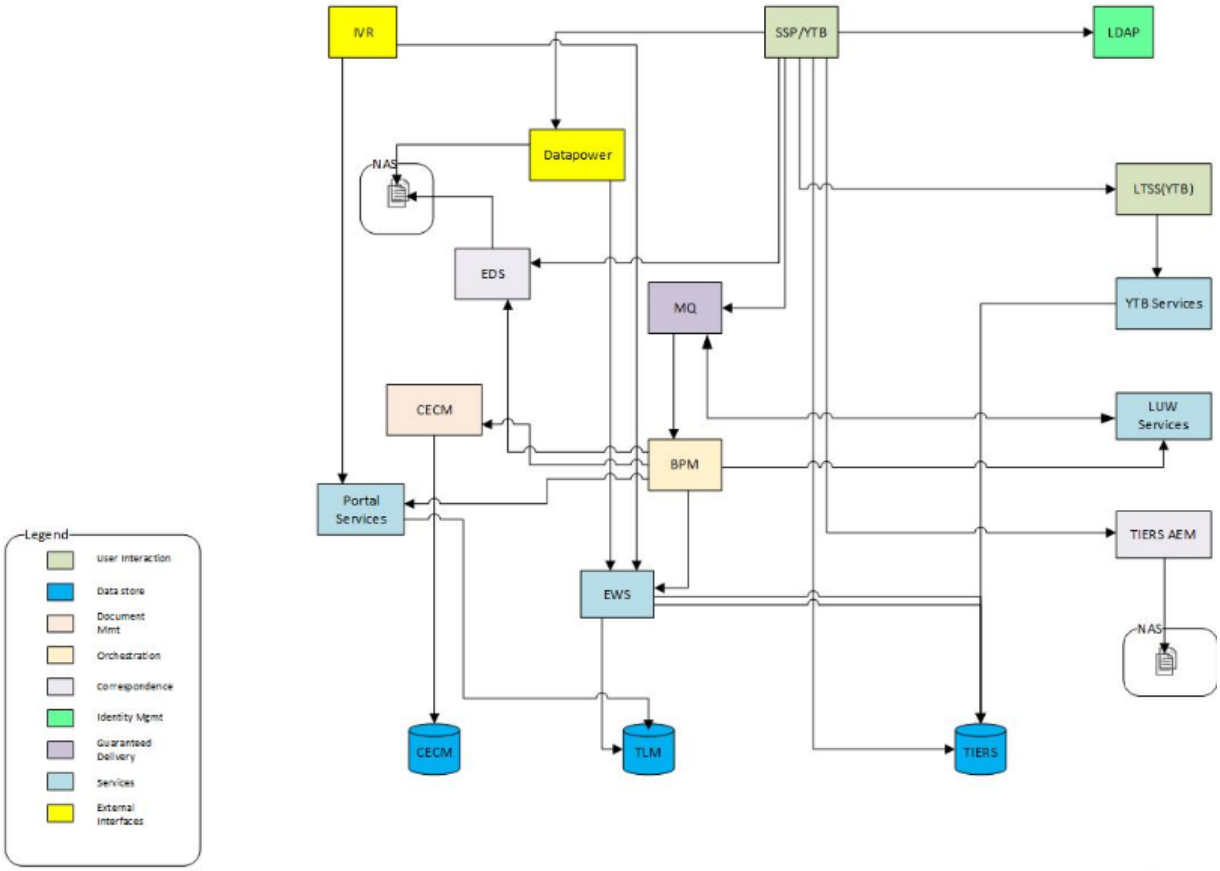
Platform	Components	Category	Security Concerns and Implemented Controls
Enterprise Content Manager (ECM)	Number of Servers: 5 ECM: 2 LiveCycle: 3 VLANs:120	Hardware	Firewalls are in place to mitigate threats from public internet; Data center has strong physical security and access controls to prevent unauthorized access.
	Java Enterprise Edition IBM Content Manager Adobe LiveCycle	Software	Like other Java applications, vulnerable to XSS and injection. Input validation and parameterized queries are implemented in addition to strong authentication via WebSeal.
Enterprise Document Services (EDS)	Number of Servers: 17 LiveCycle: 3 Kofax: 14 VLANs: 120	Hardware	Firewalls are in place to mitigate threats from public internet; Data center has strong physical security and access controls to prevent unauthorized access.
	Adobe LiveCycle	Software	n/a
Enterprise Web Services (EWS)	Number of Servers:11 VLANs:130, 163	Hardware	Firewalls in place to mitigate threats from outside world; Data center has strong physical security and access controls to prevent unauthorized access.
	Business Process Execution Language BPEL	Software	This component is located in the middleware layer. Users must be authenticated through Identity Management.
Document Center	Number of Servers: 17 VLANs: 120	Hardware	Firewalls in place to mitigate threats from public internet; Data center has strong physical

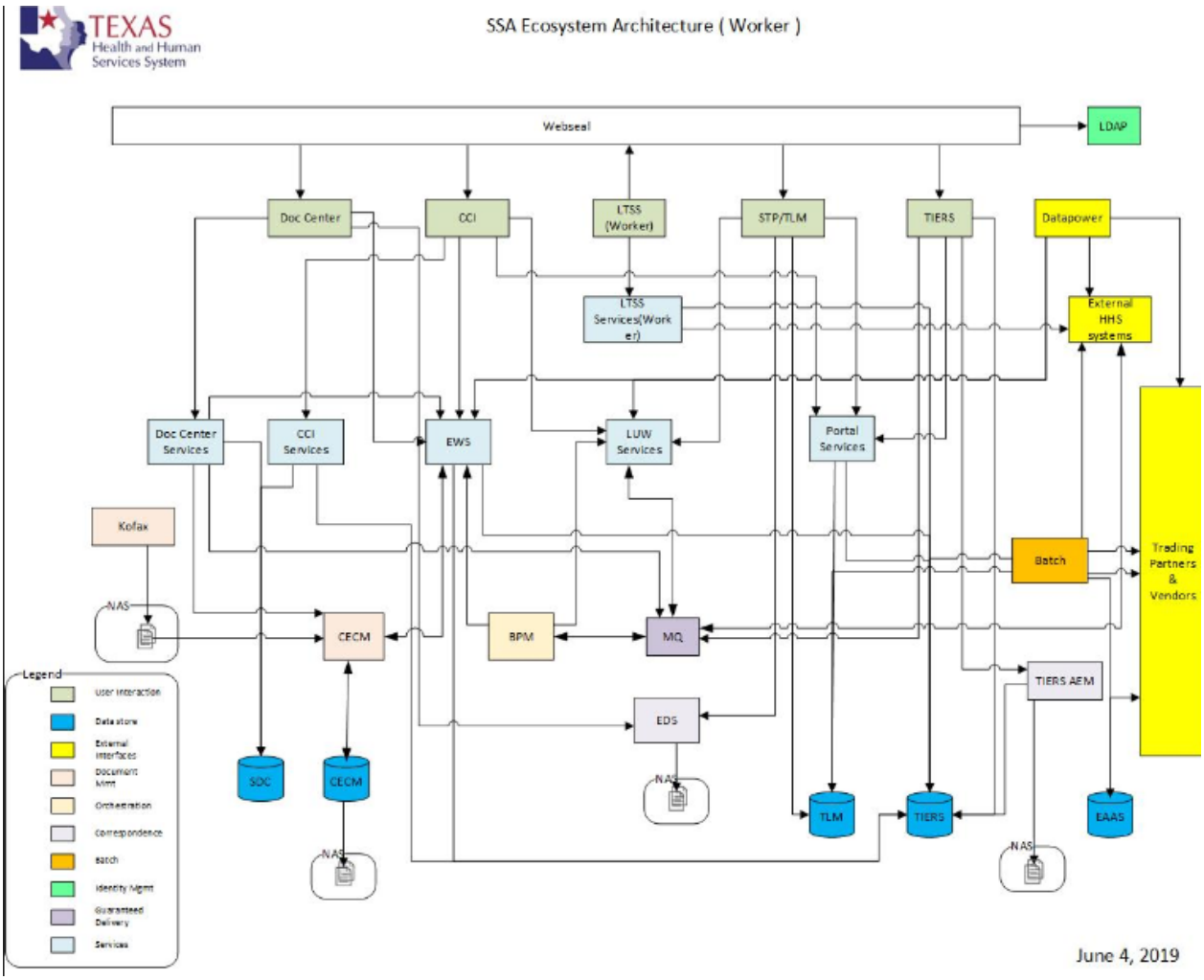
Platform	Components	Category	Security Concerns and Implemented Controls
			security and access controls.
	Java Enterprise Edition 7 Oracle	Software	Users must first be authenticated through Identity Management.
Network Connectivity	Cisco ACS 1121 V5.4, Wireless LAN Controller V7.4, Cisco 3602i AP V7.4, Cisco MSE V7.4, Cisco Prime NCS V1.3	Communications/ Wireless	Contains PII/PHI – All communications going over a public network are encrypted and sent via SFTP, HTTPS, or VPN. TIERS uses NIST-validated encryption methods.

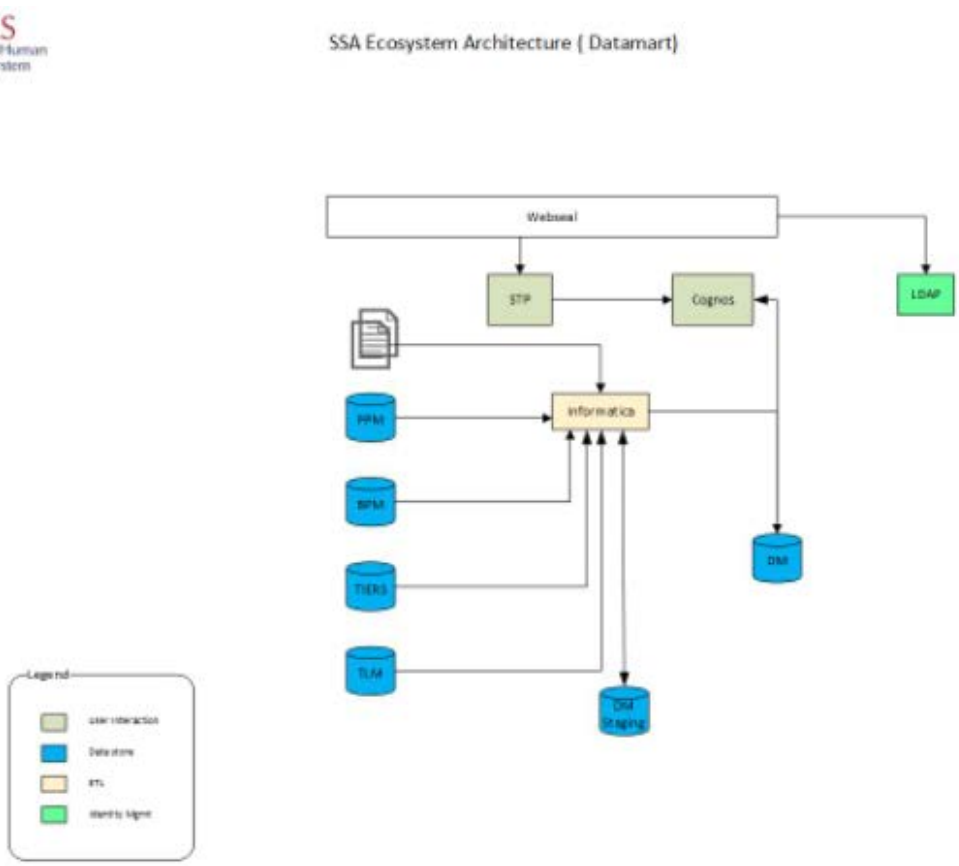
4.11 Platform Components

The diagrams starting on the next page illustrate the exiting TIERS environments:

SSA Ecosystem Architecture (Citizen)




TEXAS
Health and Human
Services System
SSA Ecosystem Architecture (Worker)
Webseal
LDAP
Doc Center
CCI
LTSS (Worker)
STP/TLM
TIERS
Datapower
LTSS Services(Worker)
External HHS systems
Doc Center Services
CCI Services
EWS
LUW Services
Portal Services
Kofax
NAS
CECM
BPM
MQ
Batch
Trading Partners & Vendors
TIERS AEM
EDS
SDC
CECM
NAS
NAS
TLM
TIERS
EAAS
NAS
Legend
User Interaction
Data store
External Interfaces
Document Mgmt
Orchestration
Correspondence
Batch
Identity Mgmt
Guaranteed Delivery
Services
June 4, 2019



5. E-Authentication Architecture, Products and Protocols

The TIERS system is a collaborative computing environment and its architecture is documented in Figure 9.

The E-Authentication architecture implemented by TIERS systems is described as follows:

The E-authentication interoperable product used is **IBM Security Identity Manager (SIM) / Security Access Manager (SAM)**.

Secure SSL/HTTPS communication is implemented from browser to backend system

Authentication is supported using IBM Security Identity Manager (SIM) / Security Access Manager (SAM) LDAP (Lightweight Directory Access Protocol) repository.

Application Security is implemented using JAAS (Java Authentication and Authorization Service) libraries and IBM LTPA

(Lightweight Third-Party Authentication) technology provided within IBM WebSphere.

The principal protocols used throughout the system include, but are not limited to: LDAP, LTPA, VIP, SOAP, HTTPS, RPC, SFTP, and SSL.

Additional advanced authentication is provided for access to client case level data by validating client identity using third party Identity and Authentication Services.

Uploaded documents are validated using Symantec Virus Scan.

Application uses secure coding practices to avoid security vulnerabilities (e.g. SQL injection, session hijacking, etc.)

5.1 Description of Customer Groups Authenticated

The following information refers to user groups that authenticate to online systems. The description in detail of these group is as follows:

5.2 Clerk

Clerks are staff members of Texas HHSC who perform administrative tasks. Eligibility Services clerks provides a variety of clerical support services in a service delivery office. Tasks may include the following:

- Providing clerical support to Texas Works Advisors staff
- Processing mail, opening and date stamping incoming applications and supporting documents
- Reviewing applications for required signature, date, and supporting documents
- Logging applications and assigning completed applications for processing
- Returning incomplete applications to clients and assisting with completion when necessary/requested
- Copying and returning original documents to clients/customers upon request
- Responding to client inquiries and requests for assistance

5.3 Supervisor

Supervisors provide guidance and instruction to clerks and observe their work. Supervisors handle more complex administrative tasks as well as management tasks.

5.4 HHSC Eligibility CSR

HHSC Eligibility Customer Service Representatives interface with customers to assist them with applying for benefits, checking the status of their benefits, updating their records, and other tasks. Work may involve interviewing clients, documenting information gathered, determining benefits, verifying case data, explaining program benefits and requirements. HHSC Eligibility Customer Service Representatives also review eligibility of clients for ongoing services.

5.5 Business Users

Business users in a Call Center and provide assistance over the phone to customers applying for benefits. Their tasks include:

- Responding to client inquiries and questions to clients calling 2-1-1
- Accepting/recording client reported changes using Self Service Portal (SSP)
- Routing and escalating complaints
- Referring callers to other phone numbers/programs/agencies when required
- Providing application and screening assistance using Self Service Portal (SSP)
- Processing requests for forms/correspondence
- Providing callers with case/benefits status
- Resolving questions about appointment status
- Rescheduling appointments using State Portal Scheduler
- Clarifying requests for missing information/verifications

5.6 Client

Client is an individual applying for benefits. A client may take the following actions:

- Completing, signing and submitting an application
- Designating a health plan
- Completing and submitting a renewal form
- Receiving notices and other communications from the agency
- Interfacing with the agency, such as reporting changes

5.7 Authorized Rep

An Authorized Representative (AR) is an individual or organization designated by an applicant or recipient to take the following actions on the applicant's behalf:

- Signing an application

Designating a health plan
Completing and submitting a renewal form
Receiving copies of the applicant's/client's notices and other communications from the agency
Acting on behalf of the applicant/client in all other matters with the agency, such as reporting changes.

5.8 CBO

A **Community-based Organization (CBO)** partners with HHSC to help people learn how they can get the most out of the HHSC's benefits application and management website, YourTexasBenefits.com. The organizations that become Community Partners represent a wide range of social services, including public entities, non-profit organizations, and faith-based groups. An organization interested in becoming a Community Partner enrolls by submitting an Interest Form online, which includes questions on what Community Partner level the organization is best suited for. Once enrolled, HHSC then provides online training and certification to interested staff and volunteers of those Community Partners approved to provide one-on-one assistance with YourTexasBenefits.com. Community Partners also have access to reports from HHSC showing how many people the organization has assisted in applying for and managing HHSC benefits online at YourTexasBenefits.com.

5.9 Advisor

A Texas Works Advisor accurately determines eligibility for TANF, Food Stamps and/or Medicaid Programs. Work involves interviewing clients, documenting information gathered, determining benefits, verifying case data, explaining program benefits and requirements. Reviews eligibility of clients for ongoing services.

Attachment D: TIERS Configuration Management Plan

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Configuration Management Plan

Texas Integrated Eligibility Redesign System

Version 4.0

Document Control Information

Document Information

Document Name	Configuration Management Plan
Project Name	Texas Integrated Eligibility Redesign System – Software Development and Maintenance
Client	Texas Health and Human Services Commission
Document Author	
Document Version	4.0
Document Status	Ready for Submission
Date Released	02/15/2019

Document Edit History

Version	Date	Additions/Modifications	Prepared/Revised by
1.0	08/22/2018	Initial Submission	
2.0	09/28/2018	Second Submission	
3.0	11/14/2018	Third Submission	
4.0	2/15/2019	Fourth Submission	

Document Review/Approval History

Date	Organization/Title	Comments
08/22/2018	Deloitte Consulting	Initial Submission
09/28/2018	Deloitte Consulting	Second Submission - Updates made per HHSC Comments
11/14/2018	Deloitte Consulting	Third Submission - Updates made per HHSC follow-up comments and a final QA for language clarity, punctuation and formatting. Note: track changes in this document show all text changes since last submission, excluding formatting and punctuation updates.
2/15/2019	Deloitte Consulting	First re-submission after initial document approval Note: Track changes show all updates since document approval.

Table of Contents

1 Introduction 5

2 Overview 5

3 Configuration Items 5
3.1 Application Configuration items 5
3.2 Script Configuration Items 6
3.3 Batch Configuration Items 7
3.4 Tool Configuration Items 7
3.5 Hardware & Software Inventories 8
3.6 Documentation Configuration Items 9

4 Agile Environments 10

5 Configuration Items Repository Structure 11

6 Configuration Management Processes 11
6.1 Development Process 11
6.2 Configuration Management Environments 12
6.2.1 ClearCase Stream Structure 12
6.2.2 ClearCase Stream Usage 13
6.2.3 Access Rights 14
6.2.4 ClearCase Activity Headline 14
6.2.5 ClearQuest 15
6.2.6 Check-out Procedures 15
6.2.7 Check-in Procedures 15

7 Baseline Process 16

8 Merge Procedures 17

9 Rebase Process 17

10 Build and Deployment Process 20
10.1 Automation Build Script Change Process: 20
10.1.1 Build Scripts Management 20
10.1.2 Build Process 20
10.2 Properties 21
10.2.1 Properties Management 21
10.2.2 WebSphere Application Server Configuration (WAS) 22
10.2.3 Deployments 22
10.3 Deployment Artifacts Promotion Process 24
10.3.1 Automation Configuration Item Promotion Process: 24
10.3.2 Application Configuration Item Promotion Process: 25
10.4 Mobile application deployment and source control process 26

11 Documentation Management 32

1 Introduction

The Configuration Management Plan defines the roles, tools and processes to identify, control and maintain software Configuration Items (CIs) related to the TIERS Suite of Applications. All references to 'TIERS' in this document collectively refer to the TIERS Suite of Applications (Texas Integrated Eligibility Redesign System Module, YourTexasBenefits.com, Long Term Services and Support (LTSS) Screener, LTSS Worker Portal, and YourTexasBenefits Mobile Application), unless specifically noted.

This plan serves as the foundation for all configuration management activities including non-code related deliverables. The Configuration Management Plan describes processes to manage, control and deliver application code to test environments along with code merge with future development streams.

2 Overview

The Configuration Management Plan focuses on the, tools, processes and standards managed by Deloitte and HHSC for configuration management processes. Roles and Responsibilities of the Configuration Management Team are listed in the Project Management Plan (PMP) Section 3.4, table 6. The document defines the process by which Configuration Items will be delivered from development into various test, production and staging environments. This includes an overview of installed software and hardware inventories, tools to manage software configuration management and approaches to concurrent development code streams. This document also defines identifying and controlling configuration items such as project deliverables and artifacts for TIERS.

3 Configuration Items

This plan defines configuration items as any application source code file, build script or other resource which requires configuration management services. The primary configuration management services are version control, change management, and application build and deployment services for the Deloitte-managed TIERS Suite of Applications. This plan creates five categories of configuration items: Application Configuration Items, Script Configuration Items, Batch Configuration Items, Tool Configuration Items, and Documentation Configuration Items. Sections 3.1 - 3.6 of this document provide details and list the file types for each configuration item category for TIERS.

3.1 Application Configuration items

These items include application configuration items required, at runtime, by the online or batch application as well as scripts and migration routines used against the TIERS Database. DataSources, Activation Specification, and NameSpace Bindings were previously stored and archived under BMC Middleware Automation (BMC) products. These legacy BMA application configuration files are now managed in IBM ClearCase.

- DDL/Build Script files are managed by the Deloitte DBA Team in a Database Tools server.
- DMLs for reference table data is maintained along with source code as (.dat) files and are managed in every release by the Deloitte Framework Team.
- Functional and Performance Test automation scripts are stored in HP Application Lifecycle Management (HP-ALM) and are executed from HP Unified Functional Testing (HP UFT) tools.
- Mobile application configuration items are stored in ClearCase.

The following table describes the Application Configuration Item file types.

Online Application File Types	File Extension
Enterprise Java Beans (EJB)	[.java]
EJB Deployment Descriptors	[.xml]
Plain Old Java Objects (POJO)	[.java]
Java Servlets	[.java]
Application Configuration Files	[.xml]
Portal Configuration Files	[.xml]
Data File	[.dat]
Property Files	[.properties]
JavaServer Pages (JSP)	[.jsp]
HTML Files	[.html]
Style Sheets (CSS)	[.css]
JavaScript	[.js]
Images	[.gif, .jpeg]
Rules Engine Decision Tables	[.xml] [.xls]
Document Type Definitions (DTD)	[.dtd]
Application Deployment Descriptors	[.xml]
WebSphere Extensions	[.xmi]
Third-Party JAR Files	[.jar]
Report Files	[.rpt]
WS Files	[.xsd/.wsd]

Table 1: Application Configuration Item file types

Note: The war and ear files are generated dynamically and packaged by the build scripts.

3.2 Script Configuration Items

These items include scripts used to compile, package, assemble and deploy to the TIERS Suite of Applications. These scripts include Apache Maven, Apache Ant, Perl, Rational Perl and Shell scripts.

The following table describes the Script Configuration Item file types.

Script File Type	File Extension
Apache Ant, Maven Build files Property Files	[.xml] [.properties]
Tcl/Java Scripts	[.jacl]
Shell Scripts	[.sh] / [.ksh]
Perl Scripts Third- Party JAR Files Database Query Files	[.pl] [.jar] [.sql]
Mercury LoadRunner Scripts	[.c]
Mercury LoadRunner Paramerter Files	[.cvs]
Mercury LoadRunner Configuration Files	[.prm, .usr]
Mercury LoadRunner Results Archives	[.zip]

Table 2: Script Configuration Item file types

3.3 Batch Configuration Items

These items include file types that are used for executing Batch, such as Shell Scripts, Property Files and Third-Party JAR Files.

The following table describes the Batch Configuration Item file types.

Batch File Type	File Extension
Plain Old Java Objects (POJO)	[.java]
Shell Scripts	[.ksh]
Application Configuration Files	[.xml]
Property Files	[.properties]
Third-Party JAR Files	[.jar]
Correspondence Templates	[.prn]
Batch Application Java Archive	[.jar]
XML Schema Definition	[.xsd]
Document Type Definitions (DTD)	[.dtd]
Shell Scripts	[.sh]

Table 3: Batch Configuration Item file types

3.4 Tool Configuration Items

Tool configuration items are used during the Build and Deployment processes. These items include tool Configuration files and Staging scripts. Examples of these Tool Configuration Items

include Apache Ant, Perl, Rational Perl, and Shell Scripts. The following table lists each Tool Configuration item.

Tool Script Types	File Extension
Apache Ant	[.xml]
Perl, Rational Perl	[.pl]
Shell Scripts	[.ksh] [.sh]
Maven Scripts	[.xml]
Websphere Admin Scripts	[.sh]

Table 4: Tool Configuration Item file types

3.5 Hardware & Software Inventories

The Hardware and Software configuration items installed on the components of each environment are maintained by the HHSC Environment Management Team. The current build and deployment process is from shared UNIX environments. The following tables show the different Hardware and Software configuration items:

Hardware Tool Name	Usage Description
Linux Machine – lwtd0xx –(021/025) Redhat Enterprise Linux Server release 6.7 (Santiago) Memory Size 72504 MB	Used to execute all the build and deployment scripts of the TIERS

Table 5: Hardware Configuration Item types

Software Tool Name	Usage Description
Perl 5.10.1	Used in deployment scripts of the TIERS to deploy Reference table changes to Database
Sqlplus 10.2.0.1.0, 11.2.0.1.0	Database client tool used to execute all the commands related to Database
IBM Rational ClearCase 8.0.0.10	Software tool used for revision control of source code and other software development assets
IBM Rational ClearQuest 8.0.0.10	Rational ClearQuest is used to trace code change sets and version details in ClearCase
IBM Rational Requisite Pro 7.1.3.10	Software tool used for managing legacy requirement documentation and use case management
JIRA v1001.0.03	Software tool used for managing Sprints, tasks and story bugs
IBM Rational Application	Software IDE tool that provides optimized development for IBM middleware

Developer Developer 8.5.5.0, 9.6.1	
IBM Rational Solution Architect 7.5.5	Software IDE tool for modeling, developing, analyzing, and verifying software applications in multiple programming languages
IBM WebSphere wsadmin tool (Jacl & Jython)	Tool utilized along with WebSphere
Oracle Database Server (11g version 11.2.0.3.0)	Database server used for TIERS
Oracle Database Server (12c version 11.2.0.3.0)	Database server used for TIERS for compatibly testing.
CA Erwin Release 9.8	Data modeling tool used by DBAs to create and maintain data models
PL/SQL Developer version 11	GUI tool to access Oracle database used by DBAs and Developers
TOAD version 13.1	Database Administration tool used by Oracle DBAs
Apache Ant (1.6.3)	Deployment tool used in the TIERS deployment process
Shell Scripts (BASH Shell)	Operating system shell
Perl and Rational Perl 5.8	Scripting language used in the TIERS build and deployment process along with other tools
Apache Maven 2.2.1	Engine used for compiling and packaging the Deloitte managed application code
Jenkins 2.142	Jenkins is an open source automation server used for continuous delivery
IBM WebSphere Application Server 8.5.5 / 8.5.5.13	J2EE Application server that hosts the TIERS for online and webservices applications
IBM WebSphere Portal 8.0, 8.5.0	WebSphere Portal Server that hosts BIP LTSS applications

Table 6: Software Configuration Item types

3.6 Documentation Configuration Items

Documentation Configuration Items are deliverables which include (but are not limited to) the Project Management Plan and Performance and Quality Management Plan. For a full list of documentation configuration items, please refer to the Change Management Plan Section 6.1.

The documentation file types seen in the table below are used to track process workflow changes for the TIERS managed applications. These files are version controlled under the DC_Projects project VOB in ClearCase.

Documentation File Types in ClearCase	File Extension
Business Process Model	[.bpmn]
Decision Tables	[.xls]

UML Document	[.emx]

Table 7: Documentation file types in ClearCase

The documentation file types seen in the table below are used to track document deliverables. These files are versioned in the SharePoint document storage management system.

Documentation File Types in SharePoint	File Extension
Document deliverables, such as Project Management Plan, Performance and Quality Management Plan etc.	[.doc] [.xlsx]

Table 8: Documentation file types in Share Point

The following files are stored in a release-specific shared file folder.

Documentation File Types in Project Share File Directory	File Extension
Data Dictionary	[.doc]
Data Model/ERD Diagram	[.er1]

Table 9: Documentation file types in Project Share File Directory

4 Agile Environments

The TIERS environment and stream structure are based on the dynamic delivery options that Agile demands. As flexibility is inserted into the process, it is done with constant consideration for the complexity of the integrated applications that HHSC maintains. During the build process, application binaries are generated along with application-specific configurations, such as database reference related scripts, and deployment scripts for specific application development, enhancement, and maintenance efforts. During the build process, the Deloitte Configuration Management team creates packages that are tagged with baselines that contain application binaries, database reference scripts, deployment scripts, and application-specific configuration items. To add the needed flexibility, planning and controls are included in the delivery process. Refer to Test Management Plan, Section 11 for details regarding Environments for development and testing.

5 Configuration Items Repository Structure

Rational UCM ClearCase provides version control services for configuration items such as application source code, database reference tables, application configurations, and build and deployments scripts. SharePoint is used as the Configuration Management tool to manage Project Management process documentation.

The Configuration Management Team structures the ClearCase installation to maximize productivity of all team members requiring its services. The ClearCase implementation and structure is subject to change as project requirements evolve and new implementation approaches are adapted. The Configuration Management Team will revise this plan to capture any changes to ClearCase and the repository structure.

Configuration status accounting is performed by using HP Project and Portfolio Management (HP-PPM) and Remedy Tools as well as storage tools such as ClearCase. HP-PPM, JIRA and Jama are used to plan, track, and support Agile artifact documentation.

6 Configuration Management Processes

IBM's Unified Change Management (UCM) best practices are followed as guidelines in the configuration management process. The following sections discuss the key processes, roles and responsibilities which support application development and delivery.

6.1 Development Process

The Development Process for TIERS follows the SDLC defined in the TIERS Software Specifications Standards and Guidelines (SSS&G). This approach is supported through ClearCase stream structure and automated build processes. The ClearCase stream structure defined in this document supports the TIERS Suite of Applications.

The Configuration Management process defined in Section 6.2 applies to application source code, database reference table data, and build scripts. Release-specific Database build script files are developed and managed in a shared location on the Database Tools server. Functional and Performance Test automation scripts are stored in HP Application Lifecycle Management (HP-ALM) and are executed from HP-UFT tools. Mobile application configuration items are stored in ClearCase.

The following Change Management strategies are also defined in the section below:

- Check-out Procedures
- Check-in Procedures Baseline Process
- Merge Procedures

- Rebase Process

6.2 Configuration Management Environments

The Configuration Management Team manages application deployments on iDEV environments for TIERS Online, TIERS Batch, YourTexasBenefits.com, YourTexasBenefitsMobile App, LTSS Citizen Portal, and LTSS Worker Portal. Rational ClearCase is the primary tool which facilitates configuration management for the various TIERS environments. The Deloitte Team members use Rational ClearCase to place Configuration Items (CI) under version control and track all revisions. The methodology used by Deloitte's Configuration Management Team follows IBM's UCM best practices. The stream structure implemented in ClearCase defines how team members work with ClearCase and how the development process is implemented with the help of configuration management tools.

6.2.1 ClearCase Stream Structure

This section defines the Rational ClearCase stream structure used to manage all the TIERS Project CI's. The TIERS project utilizes parallel stream development with a hierarchical stream structure. This section will be updated regularly by Deloitte as the stream structure changes.

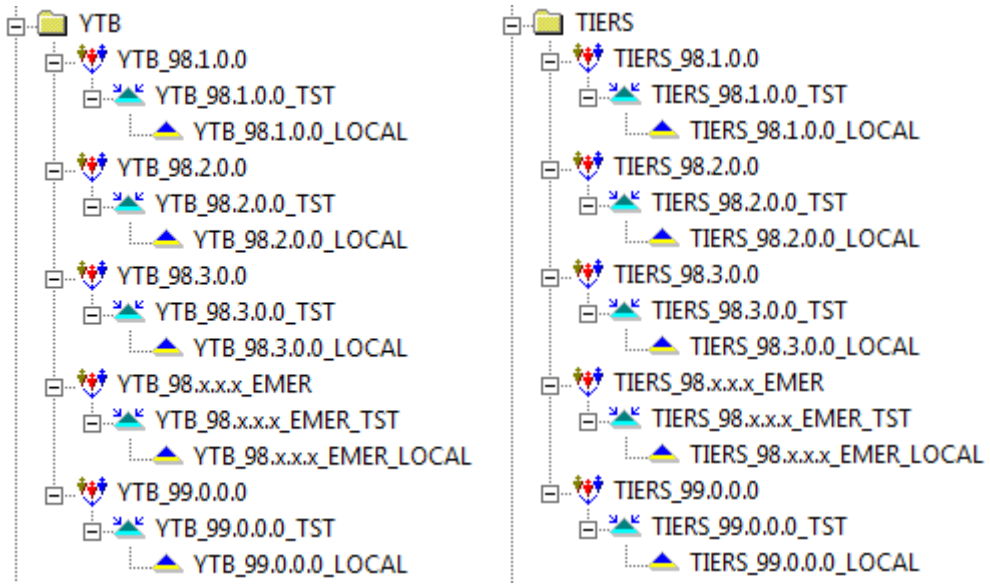


Figure 1: ClearCase Stream Structure

The stream is organized according to the various stages of development and testing within each release. New ClearCase projects will be created for every release e.g. 99.0, 99.1.

These projects are reused for all emergency releases for the duration of a cycle set. For example, 99.X.X.X will be reused for all Emergency releases between 99.0 and 100.0.

6.2.2 ClearCase Stream Usage

- Each project created for a release contains an integration stream called <Project> _<ReleaseNumber>_TST stream and has one stream under it; <Project>_<ReleaseNumber>_LOCAL, where <ReleaseNumber> is the release number e.g. 99.0.0.0 and Project is either TIERS, YTB, BIP_LTSS and SSP_Mobile.

- The TIERS <ReleaseNumber>_LOCAL, YTB_<ReleaseNumber>_LOCAL, BIP_LTSS_<ReleaseNumber>_LOCAL, SSP_Mobile_<ReleaseNumber>_LOCAL: These streams are used by developers to develop code for a specific release. All developers have access to check-in/check-out code from these streams. A few developers chosen by Scrum Masters for each functional area manage the responsibility of delivering activities to TIERS_<ReleaseNumber>_TST, YTB_<ReleaseNumber>_TST, BIP_LTSS_<ReleaseNumber>_TST, and SSP_Mobile_<ReleaseNumber>_TST.

- The TIERS _<ReleaseNumber>_TST, YTB_<ReleaseNumber>_TST, BIP_LTSS_<ReleaseNumber>_TST, and SSP_Mobile_<ReleaseNumber>_TST: These streams serve as the integration streams for TIERS <ReleaseNumber>_LOCAL, YTB_<ReleaseNumber>_LOCAL, BIP_LTSS_<ReleaseNumber>_LOCAL, and SSP_Mobile. Check-in/check-outs are disallowed in the Integration (TST) streams. Baselines are created in these streams during each DEV build.

- The Emergency releases do not follow the same iDEV-iTest-Prodfix cycle of testing, hence projects created for releases only contain TIERS <Emer/SprintRelease Num>_TST, TIERS <Emer/ Release Num>_LOCAL, YTB< Emer/SprintRelease Num>_TST> YTB <Emer/ Release Num>_LOCAL, BIP_LTSS< Emer/SprintRelease Num>_TST> BIP_LTSS <Emer/ Release Num>_LOCAL, and SSP_Mobile< Emer/SprintRelease Num>_TST> SSP_Mobile <Emer/ Release Num>_LOCAL.

- The TIERS <EmerReleaseNumber>_LOCAL, YTB <EmerReleaseNumber>_LOCAL, BIP_LTSS <EmerReleaseNumber>_LOCAL and SSP_Mobile <EmerReleaseNumber>_LOCAL: These streams are used by developers to develop code for a release. All developers have access to check-in/check-out code from these streams. A few developers chosen by the Scrum Masters for each Sprint will manage the responsibility of delivering activities to TIERS _<Emer/ReleaseNumber>_TST, YTB _< ReleaseNumber>_TST, BIP_LTSS _< ReleaseNumber>_TST, and SSP_Mobile_< ReleaseNumber>_TST.

- The TIERS _<EmerReleaseNumber>_TST, YTB _<EmerReleaseNumber>_TST, BIP_LTSS <EmerReleaseNumber>_TST, and SSP_Mobile_<EmerReleaseNumber>_TST: These streams serves as integration streams to which developers deliver their activities in order to be built and deployed. Baselines are created here and rebased into TIERS _< Release Num>_TST or YTB _< Release Num>_TST streams.

- The TIERS _<EmerReleaseNumber>_TST, YTB _<EmerReleaseNumber>_TST, BIP_LTSS _<EmerReleaseNumber>_TST, and SSP_Mobile_<EmerReleaseNumber>_TST: These are read-only streams used to rebase with a baseline that is ready to be built and deployed to Prod_Fix environment for UAT testing.

- Because new projects and streams are created for different releases, it is the responsibility of the ClearCase users to create and update views as appropriate.

6.2.3 Access Rights

The table below describes user access rights and privileges to various ClearCase streams. The access is controlled by HHSC and should be designated only to the TIERS developers and leads.

Stream	Who	Access Level
TIERS _<ReleaseNumber>_LOCAL & YTB _<ReleaseNumber>_LOCAL & BIP_LTSS_<ReleaseNumber>_LOCAL & SSP_Mobile_<ReleaseNumber>_LOCAL	All members of ClearCase user group	Check in and out code from this stream. Access to add/remove/modify directories is restricted to designated members on the Framework team. All other developers do not have access to add/modify/remove directories.
	Code Management Team	Check in and out code from this stream. Add/modify/remove directories or files.
TIERS _<ReleaseNumber>_TST & YTB_<ReleaseNumber>_TST & BIP_LTSS_<ReleaseNumber>_LOCAL & SSP_Mobile_<ReleaseNumber>_LOCAL	Lead Developers	Access for deliveries
	Code Management Team Build & Deployment Team	Access for deliveries Access to create baselines

Table 10: Access Rights

6.2.4 ClearCase Activity Headline

Developers use the BaseCM Activity form in ClearCase to check-in/check-out code from ClearCase and enter the following information when they create an activity.

Field	Description
Release Number	Describes the Release Number, e.g. 85.0
Agile Team	Describes the Agile Team for which activity has been created

SR Number	Describes the request for which the change is made
Description	Brief description of change
Config Request Number	Describes the Configuration request for which the change is made
DB Request Number	Describes the Database Version for which the change is made
Sprint Cycle Number	Describes the Sprint Cycle for which the change is made
QC. or JIRA User Story Number(s):	Describes the Quality Center defect ID or JIRA User Story
Headline	Automated concatenation of all above fields

Table 11: ClearCase Activities

Note: Activities that have been delivered to the parent stream cannot be reused to make changes to code. A new activity must be created each time code changes are to be made if the activity that was previously used has already been delivered.

6.2.5 ClearQuest

Rational ClearQuest is used to trace code change sets and version details in ClearCase.

6.2.6 Check-out Procedures

In ClearCase, a reserved check-out involves locking the CIs to prevent competing changes to the same CIs before the current changes are saved in ClearCase. On the other hand, unreserved check-outs allow multiple copies of the CI to be simultaneously checked-out requiring a merge to occur at check-in. While reserved check-outs help to maintain the integrity of the CIs, they also slow down the development process, whereas unreserved check-outs speed up development time at the cost of introducing risk and complexity in merging. A new version of the CI is created during each check-out. A version tree helps to illustrate the history of changes to a CI.

Application developers are responsible for checking out CIs from ClearCase. CIs cannot be checked out of ClearCase without a ClearQuest activity. The ClearQuest record ties related ClearCase activities together to provide UCM traceability.

6.2.7 Check-in Procedures

Once changes to a CI have been completed, the CI is checked-in by the developer and unlocked in ClearCase. ClearCase has been configured to disallow reserved check-outs. Multiple check-ins of a CI may result in non-trivial merge conflicts which are resolved by the developers performing the check-in/merge. UCM pre-operational and post-operational triggers govern that check-in requirements have been met before check-in activity completes successfully.

The ClearCase check-in processes begin with the creation of a BaseCMActivity. The development team will then apply their changes to the source control system. The BaseCMActivity will create changesets for the applied changes. The Development team may complete their changes by performing a commit action.

This ClearCase check-in process applies to Application Source Codes, Database Reference Table data, and Build scripts. Release specific Database Build script files are developed and managed in a shared location on the Database Tools server. Functional and Performance Test automation scripts are stored in HP-ALM and are executed from HP-UFT tools.

7 Baseline Process

A baseline is a stable configuration of one or more components. It is a snapshot, in time, of the individual versioned object bases.

- In ClearCase, baselines are generated in the TIERS _<ReleaseNumber>_TST, YTB _<ReleaseNumber>_TST, BIP_LTSS _<ReleaseNumber>_TST, and SSP_Mobile_<ReleaseNumber>_TST integration streams.

- Database build scripts are stored on shared storage across database server. Reference data update scripts are stored in ClearCase. Functional and Performance test automation scripts are stored in HP-ALM and are executed from HP-UFT tools. Mobile application configuration items are stored in ClearCase.

- As a part of the build and deployment process, automatically, by the Jenkins automation server, baselines are also created for the purposes of rebasing code from lower to higher future release streams and these are created manually by the Configuration Management Team.

- Baseline deliveries help developers working in different release streams to stay in sync with each other's work. Each new baseline of a given stream includes any work delivered or checked into the stream since the last baseline. A ClearCase baseline identifies activities and one version of every element in one or more components.

- Baseline deliveries act to sequentially merge code changes from one project to the next. When a release is deployed into production, the HHSC Rational Team creates future release projects from the released production baseline. Future release projects and streams are no longer created from the mainline project baseline.

- If there needs to be a new baseline created for the same release, the previous baseline will be renamed and "PRD" is replaced with "TMP".

- When a new baseline needs to be created in the TST stream of future releases, the following baseline naming convention is used:
  <YYYY>-<MM>-<DD>_<APP>_< Streamname>_<ReleaseNumber> _TST
  Where YYYY-MM-DD is the date of the rebase, and <APP> is the TIERS, YTB, BIP_LTSS, and SSP_Mobile applications.

- For baselines that are created in any stream for reasons of synching up two different releases, "RC" is added at the end to indicate that it is a release candidate and not a production baseline.

- This baseline is created in the TST stream of the future release.
  <YYYY>-<MM>-<DD>_<APP>_<stream-name>_<ReleaseNumber>_RC
  Where YYYY-MM-DD is the date of the rebase, and <APP> is TIERS or YTB
  E.g. 2012-05-20_TIERS_ 85.0.0.0_RC or 2012-05-20_YTB_ 85.0.0.0_RC

- The above-mentioned baseline process applies to application source codes, database reference table scripts, application configurations, and build and deployment scripts.

- Database build scripts are associated with the source code baseline during iDev deployments.

- Functional and Performance Test automation scripts are stored in HP-ALM and are executed from HP UFT tools.

8 Merge Procedures

Merging is the process of combining the contents of two or more versions of files (text file type) or directories into a single new version. ClearCase has a merge utility to facilitate combining unreserved check-outs. Unreserved check-in(s) requires a merge to be executed as each subsequently checked-out file is checked back in to ClearCase. The merge will prompt the developer to choose between conflicting changes in the CI. Baseline deliveries will be implemented to merge code from one release point to a later release point.

9 Rebase Process

Rebasing is the process of updating the contents of a stream with code from another stream. Within the TIERS projects, rebases are used to update future releases with code from prior releases.

- Database build scripts are stored on shared storage across database servers. Reference data update scripts are stored in ClearCase. Functional and Performance test automation

scripts are stored in HP Application Lifecycle Management (HP-ALM) and are executed from HP-UFT tools. Mobile application configuration items are stored in ClearCase.

- When multiple releases are being worked on simultaneously, changes made to a release which is at an advanced stage in the SDLC must be incorporated into a release which is behind in the SDLC. Code revisions from a later release baseline are never delivered into an earlier release project. For example, a baseline from release 85.1 is never rebased into the project containing 85.0 code.
- This process keeps the developers who are working in different Sprints in sync and up to date with the latest code changes across the entire application.
- During the delivery before the rebase process, the Code Management Team uses the latest baseline in the “TST” integration stream of that given release project and then delivers the latest baseline to the next area of the future release that requires synchronization.
- Before the interproject delivery occurs, all activities in TIERS_<ReleaseNumber>_LOCAL will be delivered to "TST."
- After the baseline delivery occurs to the prospective release stream, a new baseline is created in the integration stream and then is manually rebased down to the TIERS_<ReleaseNumber>_LOCAL, stream.
- The above-mentioned process applies to application source codes, database reference table scripts, application configurations, and build and deployment scripts.
- Database build scripts are applied incrementally using a custom in-house tool.
- Functional and Performance Test automation scripts are stored in HP-ALM and are executed from HP UFT tools.

Figure 2 depicts the logical flow of source code during delivery and rebase operations. The Configuration Management Team manages and executes all deliveries and rebases at levels above DEV.

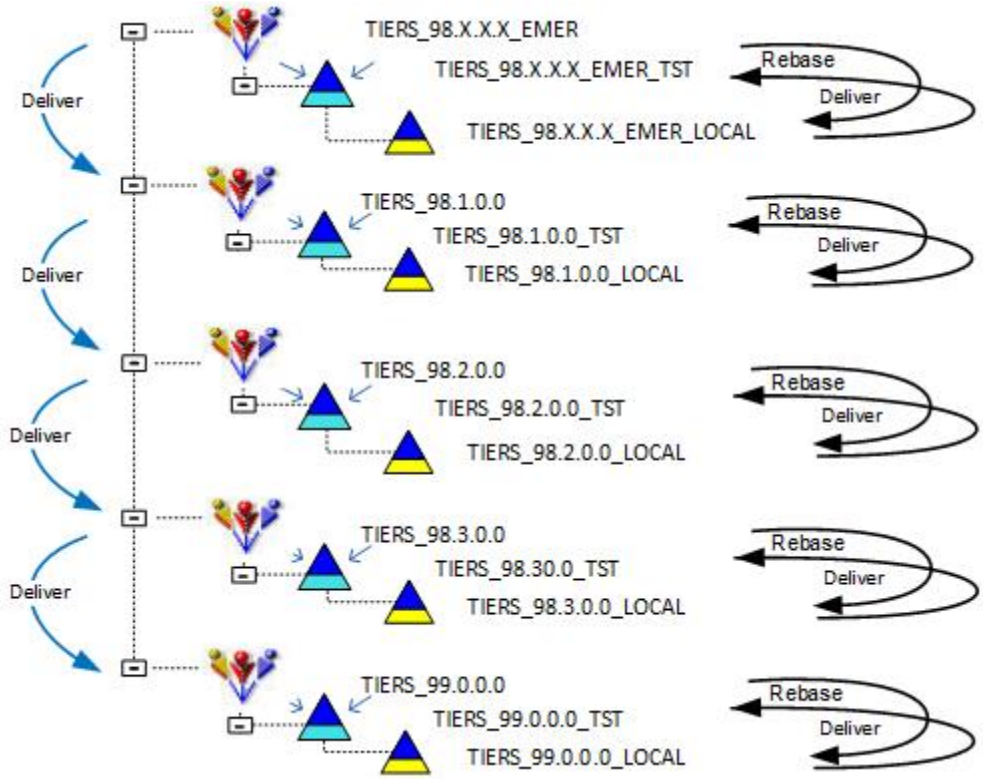


Figure 2 - Rebase Operation

10 Build and Deployment Process

A build and deployment system compiles, packages, assembles, and deploys the application along with MRS database changes and configuration items in each stream. This system is implemented as a Maven, Apache Ant Build file and a collection of external scripts and third-party services. Application builds scheduled in advance are done via the Jenkins automation server. Ad-hoc or unscheduled builds are also kicked off from the Jenkins automation server and executed with no further manual intervention. The build and deployment processes are intended to be automated; however, unforeseen circumstances may require manual intervention which, when required, is documented in the Remedy CRQ for the build.

For all environments, the build system notifies all interested parties of the success or failure of each build via email. In the event of an unsuccessful build, the build system sends compilation logs containing detailed reference(s) to the class and exception that caused the failure. At this point, the build team works with appropriate members of the development team to address the compilation issue and execute a clean build. The build scripts, streams and environments are configured to function independently. The build and deployment process is independent of the stream or application server where it deploys but rather on the environment.

10.1 Automation Build Script Change Process:

1. Automation Script changes can be initiated by either Deloitte or HHSC.
2. Script Changes are tracked using JIRA/ALM- available to both the TBT and EM teams.
3. Script changes may be necessary because of either a source code change or a general enhancement to the script.
4. For any script change/fixes, the defect will be assigned to TBT. However, if the change is included in the property files, then it will be assigned based on the ownership of the environments: lower environments to TBT and higher environments to the EM team.

10.1.1 Build Scripts Management

Deloitte is responsible for managing the Build scripts in the TIERS code stream. These scripts are packaged along with application binaries and staged for environment deployments.

10.1.2 Build Process

All Deloitte-managed application builds are handled by the Deloitte Build team. Automated builds and deployments are executed from the Jenkins automation server. The build process involves making a baseline in the TST stream of the release, updating the ClearCase view to download the latest code from ClearCase stream, and compiling the code. Application binaries, database reference tables and application configurations are packaged and staged in a directory as a tar file with the baseline name. This packaged code is then deployed to the appropriate environment as part of the deployment process execution. The table below describes the Jenkins plugins used in the build and deployment automation process.

Jenkins Plugin Name	Description
Blue Ocean	BlueOcean Aggregator
Build Pipeline	Renders upstream and downstream connected jobs that typically form a build pipeline. In addition, it offers the ability to define manual triggers for jobs that require intervention prior to execution, e.g. an approval process outside of Jenkins.
Build With Parameters	Allows the user to provide parameters for a build in the url (similar to /job/JOBNAME/buildWithParameters), prompting for confirmation before triggering the job.
Extensible Choice Parameter plugin	Provides several ways to retrieve choices, including the way to share choices among all jobs.
HP-ALM Quality Center Plugin	HP Quality Center Plugin
Mail Watcher Plugin	Notifies configured email recipients on various events.
Parameterized Scheduler	Configures a cron style timer schedule for parameterized builds.
Publish Over SSH	End build artifacts over SSH
jobConfigHistory	Saves a copy of the configuration file of a job (config.xml) for every change made and of the system configuration.
Zentimestamp	Adds timestamps to console output
Timestamper	Adds timestamps to console output

Table 12: Jenkins Plugin names and description

Database builds are created by the Deloitte DBA and stored at a shared location in the DB Tools Server. Functional and Performance Test automation scripts are stored in HP-ALM and are executed from HP-UFT tools.

10.2 Properties

10.2.1 Properties Management

Property files are managed in ClearCase under TIERS_CFG_<release_number>_LOCAL, YTB_CFG_<release_number>_LOCAL, BIP_LTSS_CFG_<release_number>_LOCAL streams within the TIERS_Config_Lower, YTB_Config_Lower, and BIP_LTSS_Lower Projects. All Deloitte-controlled environment property changes are made by the Deloitte Build Team in <TIERS/YTB/BIP_LTSS>_Config_Lower projects and all HHSC-controlled environment property changes are made by the HHSC environment management team in <TIERS/YTB/BIP_LTSS>_Config_Upper project. The properties related to build and

deployment processes are managed under tclw/bmw/build VOB. The properties related to environments and referenced by application code are managed under tclw/props VOB for TIERS, ytblw/props for YTB, dcbplw/props for DC_BIP which follow the application configuration item promotion process defined in "Application Configuration Item Promotion Process." The diagram below describes the stream structure used for properties.

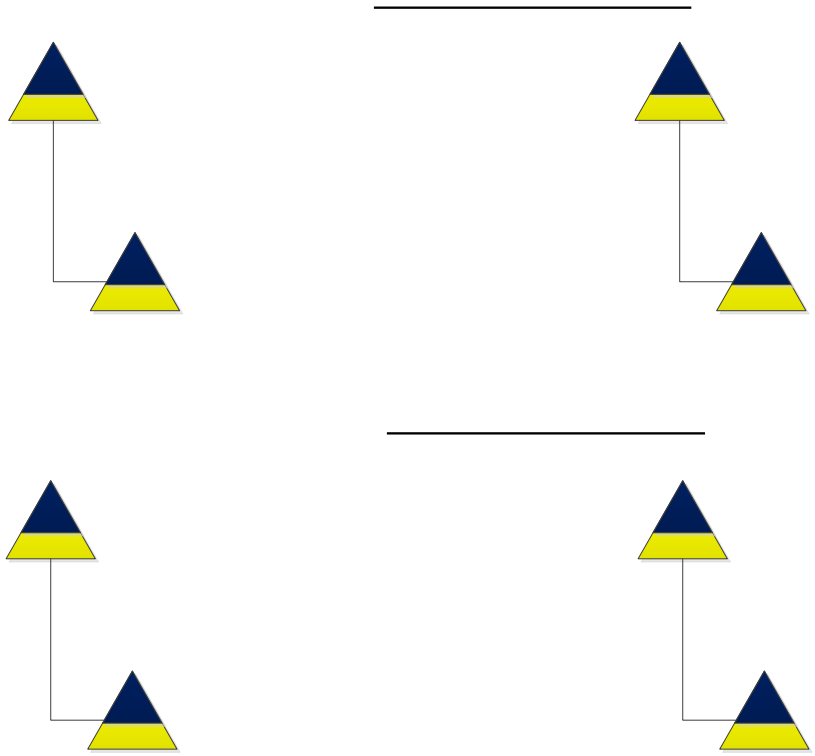


Figure 3 - New Structure for Property Files Management

10.2.2 WebSphere Application Server Configuration (WAS)

Deloitte is responsible for monitoring WAS configuration changes for iDEV environments. HHSC is responsible for developing and maintaining WAS configuration changes for all other environments. The WAS configurations related to build and deployment artifacts are managed using the automation configuration item promotion process defined in section 10.3.1.

10.2.3 Deployments

Deployment script files are managed in ClearCase under <App>_<release_number>_<Code Stream> in the Deloitte managed LW_Config project. The tclw/bmw VOB is used to store Deployment scripts for TIERS, DC_YTB ytblw VOB for YTB, and DC_BIP/dcbplw for BIP_LTSS VOB.

Build scripts baselines will be made in <App>_<release_number>_<Code Stream> Integration streams. HHSC will create views from <App>_<release_number>_<Code Stream> to receive build script changes for iDEV environments deployed by Deloitte.

The stream structure shown below is used to manage build and deployment scripts.

Figure 4 - New Structure for Build & Deployment Scripts Management

The deployment scripts are managed using the automation script promotion process.

Execution

The build process is followed by staging and deployment. Staging involves creating a binary file for TIERS (online, batch, property files) code, Master Reference Schema (MRS), Crystal Reports, WebServices (online, property files) code and for YTB (Application, CR, Services, Properties) code.

Deployment involves passing the baseline as an argument to deployment scripts, extracting the staged artifact and then deploying to respective environments. Environment-specific properties are deployed from Deloitte-managed Config VOBs. During iDev deployments, code baselines are tagged with database build numbers and stored in a <ReleaseNumber>.properties at the staging location. Later, this file will be referenced to identify the required database builds for the baseline that is being deployed to higher environments. Automated smoke tests will be executed after successful deployments into environments. Functional and Performance tests are executed upon different schedules after the successful deployment to environments.

The following naming conventions are used for the directory structure of online deployment: /export2/was7/app<ENV>/profiles/<NODE>/installedApps.

Note: ENV Names are changed as part of the Agile name change Sprint/User Story to iDEV and iTest environments. ENV is the environment name, e.g., idev/itest/prod, while <NODE> will be the node name, e.g., node01/node02.

The following naming conventions are used for the directory structure of batch deployment: /TIERS /<ENV>, where ENV is the environment name.

The following naming convention is followed for the Property file stream directories for online and batch property files:

- tclw/props/TIERS/online/<ENV>
- tclw/props/TIERS/batch/<ENV>
- ytblw/props/ <ENV>
- dcbplw/props/<ENV>

In each naming convention, ENV is the environment name, e.g., /iDEV1.

10.3 Deployment Artifacts Promotion Process

The following processes are followed for Build and Deployment automation artifacts.

1. Deloitte develops and maintains automation scripts in the LOCAL streams for the environments managed by Deloitte. HHSC develops and maintains the automation scripts for the environments managed by HHSC.
2. As the release code is delivered into the HHSC-managed environments, so are the automation scripts. This is facilitated through:
    a. Deloitte promoting the scripts from LOCAL to TST and working with HHSC on resolving any merge conflicts.
    b. Deloitte changing the status of the associated SR to “Pending Deploy” and assigning it to the Environment Management Build/Deploy Lead. This will formally notify HHSC that the scripts have been promoted to TST. HHSC will review the promoted script(s) and work with Deloitte to resolve any questions.
3. HHSC will use the TST stream scripts and Jenkins automation server and environment variables to conduct an initial deployment into an environment for which they are responsible.
4. Deployment Change Process:
    a. For any script change/fixes, the defect will be assigned to TBT. However, if the change is included in the property files, then it will be assigned based on the ownership of the environments: lower environments to TBT and higher environments to the EM team.

10.3.1 Automation Configuration Item Promotion Process:

1. This process is applicable to all script-related configuration items not delivered from the LOCAL to TST stream by the Deloitte. Some examples include:
    a. WAS Configuration changes
    b. Jenkins is used for both builds and deployments
2. Deloitte develops and maintains configuration items for the environments for which they are responsible, and HHSC develops and maintains configuration items for the environments for which they are responsible. As the release code is delivered into the HHSC-managed environments, so are the configuration items. This is facilitated through the following process:

a) Deloitte updates the status of the associated change facilitated by HHSC Change Tracker Tool (CTT). This will formally notify HHSC that the scripts have been promoted to TST.
b) This CTT handoff process may continue until Environment Management changes the status to "Deployment Approved." The Environment Management Build/Deploy Lead will change the CTT statuses to "Deployment Approved" upon initial deployment to an environment for which they are responsible.
c) Also, when the CTT is in "Deployment Approved" status, any required manual updates will be approved and managed by Environment Management Team Lead.
d) Once changes are deployed into Production, the Environment Management Build/Deploy Lead will change the SR statuses to "Deployment Verified."

3. HHSC will conduct an initial deployment into an environment for which they are responsible.
   a) Deployment failures will be handled as follows:
      I. Failures due to faulty configuration item changes will be documented through a HP-ALM defect and assigned to the Environment Management Team.
      II. Defect workarounds will be jointly reviewed and approved by Deloitte and the Environment Management Team.
   b) When deployment is successful, the HHSC Environment Management Team will update the associated defect status to "Deployment Approved."

10.3.2 Application Configuration Item Promotion Process:

1. This process is applicable to all application-related configuration items not delivered from the LOCAL to TST stream by Deloitte. Some examples include:
   I. Environment-specific Property File changes
   II. WAS configuration changes
2. Deloitte develops and maintains configuration items for the environments for which they are responsible, and HHSC develops and maintains the configuration items for the environments for which HHSC is responsible.
3. As the Sprint release code is delivered into the HHSC-managed environments (iTest and above), so are the configuration items.
   a. This will be facilitated through:
      i. Deloitte creating an Environment Request (ER) and completing the Change Details section of the ER.
      ii. ER is assigned to "Environment Management" Team.
      iii. HHSC will conduct an initial deployment into an environment for which they are responsible.
   b. Deployment failures will be handled as follows:
      i. Any needed assistance will be provided by the Environment Management Team.

ii. Failures due to faulty configuration item changes will be documented through a (HP-ALM) defect and assigned to the Environment Management Team.
iii. Defect workarounds will be jointly reviewed and approved by Deloitte and Environment Management Team.

c. When deployment is successful, the HHSC Environment Management Team will mark the promotion ER complete.
    a. Please refer to Test Management Plan, Section 11 Test Environments for details regarding environment management ownership.

10.4 Mobile Application Deployment and Source Control Process

The mobile application source code is managed on the Git-based SCM using Git Flow paradigm. At the end of each Sprint, the mobile application code is checked into the HHSC ClearCase source code management system. Development and Test builds of the mobile application are deployed to HockeyApp for testing purposes. Builds for higher environments are created by the Environment Management (EM) team upon request. Once ready for Production, the latest code is configured with the Production configuration and the final build is tested for prod login and doc upload. The build is uploaded for review to the respective App Stores. On the launch date, a phased rollout to 25% of Android users is started by HHSC. Logs are monitored throughout the day to ensure there are no issues. iOS phased rollout is performed if available. Android is increased to 100% of users by HHSC.

For day-to-day development, the YTB mobile repository uses a hosted Git solution located within the Deloitte development practice, however iTEST and production builds are conducted by HHSC. HHSC currently uses IBM Rational ClearCase as its code repository. Mobile team source code deployment procedures to ClearCase enable commits for major milestones from the Git repository to ClearCase, e.g., End of Sprint, iTEST builds, and Production ready.

The mobile team creates and uses ClearCase BaseCM Activity in the SSP_Mobile release project contained under the DC_Projects PVOB in ClearCase Project Explorer to check-in source code exported from Deloitte's Git repository by executing the Cleartool ClearFSImport command in ClearCase. Code is only checked in after completing a major milestone of the release. After the code import is concluded into the SSP_Mobile LOCAL stream, the Mobile team then delivers all code changes contained in the LOCAL stream activity to SSP_Mobile_TST Integration stream. After the delivery is concluded from SSP_Mobile LOCAL stream to SSP_Mobile_TST stream, a baseline is created and then recommended in SSP_Mobile_TST stream to record a specific stage or version of its development.

The process is outlined in the section below:

Figure 5 Git Interface

- Tag the master branch with this format: “<Upper env>-Build-MMDDYYYY” – Where Upper env is iTEST1, iTEST2, etc.
- Open archive utility and zip the repository.
- Either through a share or upload/download, move the archived code repository onto the VM or physical machine.
- Decompress the folder.
- Create Activity: Open the ClearCase Explorer inside the IBM Rational ClearCase folder.

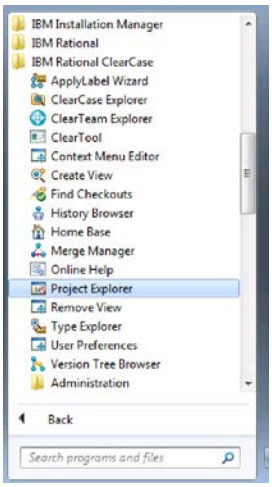


Figure 6 Navigation to Project Explorer

- Right click on the left pane and select ‘Add View Shortcut.’

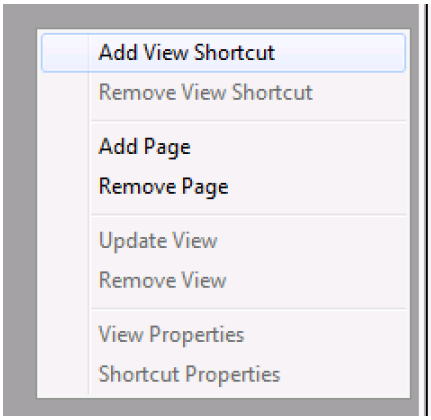


Figure 7 Selecting Shortcut View

- Select the dynamic for the 'View Type', select your local view in the 'View Tag' drop down, and make sure '{none}' is in the drop down. Select 'OK.'
- Select the newly created view shortcut, right click on the top most item, and select 'Properties of View.'

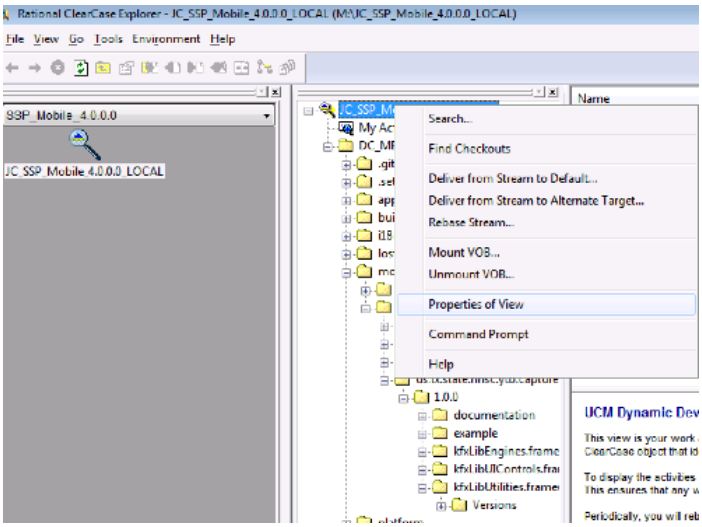


Figure 8 Properties of View under IBM Rational ClearCase Explorer

- In the general tab, select 'Change' in the activity section.

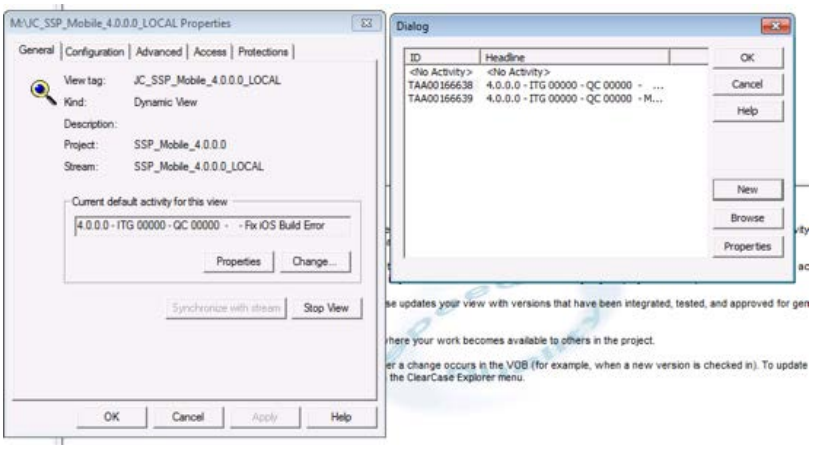


Figure 9 Change Action to create BaseCMActivity

- Select 'New' -> 'BaseCMActivity…'
- Add the release number, put '00000' for the QC and SR numbers, and fill in the descriptions. After that, select 'OK.'
- You should now see your newly created activity in 'My Activities.'

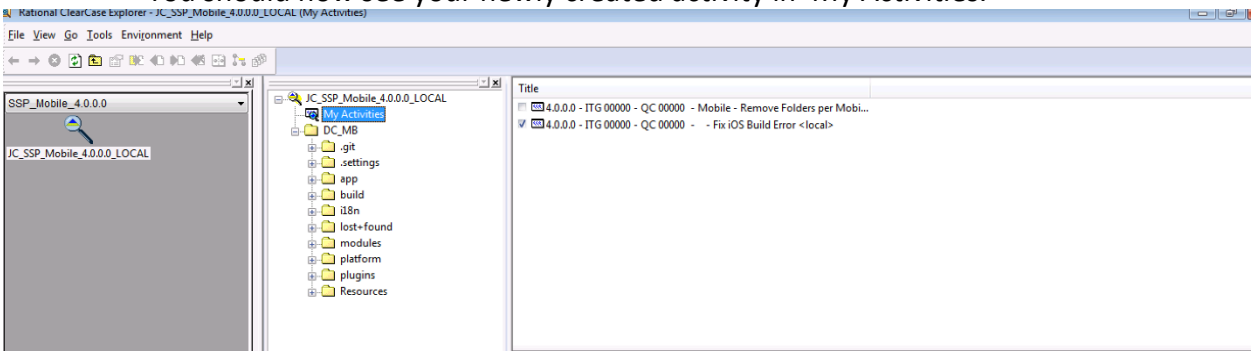


Figure 10 ClearCase explorer View panel

Import Files

- Open up a command prompt and type the command clearfsimport -preview -rec -nset PATH_TO_UNCOMPRESSED_FOLDER* PATH_TO_LOCAL_VIEW. Ensure there are no errors and the path is correct and the files are correctly imported.

```
M:\JC_SSP_Mobile_4.0.0.0_LOCAL\DC_MB>clearfsimport -preview -rec -nset c:\Users\
jceaser01\ytb\* M:\JC_SSP_Mobile_4.0.0.0_LOCAL\DC_MB_
```

Figure 11 Command prompt to initiate preview for clearfsimport

- Next, run the command clearfsimport -rec -nset PATH_TO_UNCOMPRESSED_FOLDER* PATH_TO_LOCAL_VIEW

```
M:\JC_SSP_Mobile_4.0.0.0_LOCAL\DC_MB>clearfsimport -rec -nset c:\Users\jceaser01
\ytb\* M:\JC_SSP_Mobile_4.0.0.0_LOCAL\DC_MB_
```

Figure 12 Command prompt to initiate clearfsimport

Deliver Stream

- Open the Project Explorer inside the IBM Rational ClearCase folder.
- Next, expand the DC_Projects -> SSP_Mobile -> SSP_Mobile_VERSION -> SSP_Mobile_VERSION_TST -> SSP_Mobile_VERSION_LOCAL
- Right click on SSP_Mobile_VERSION_LOCAL and select 'Deliver from Stream' -> 'To Default…' Select your activity and press 'OK.'

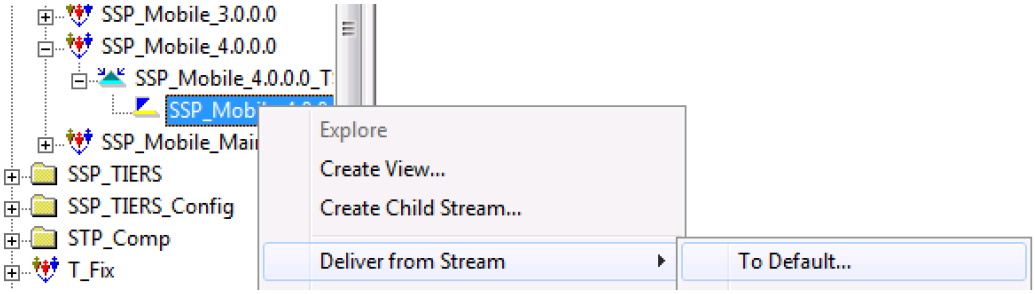


Figure 13 Deliver Activities from Local to TST Stream

- Once this is complete, scan the logs for errors. If there are no errors, you MUST select 'Complete.'

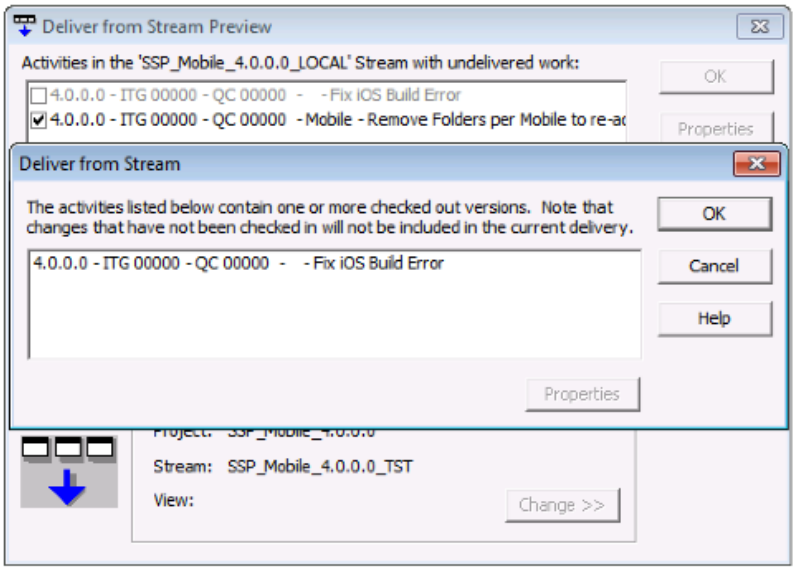


Figure 14 Activity Deliver Complete

Make Baseline

- Open the Project Explorer inside the IBM Rational ClearCase folder.
- Next, expand the DC_Projects -> SSP_Mobile -> SSP_Mobile_VERSION -> SSP_Mobile_VERSION_TST -> SSP_Mobile_VERSION_LOCAL
- Right click on SSP_Mobile_VERSION_TST and select 'Make Baseline…'

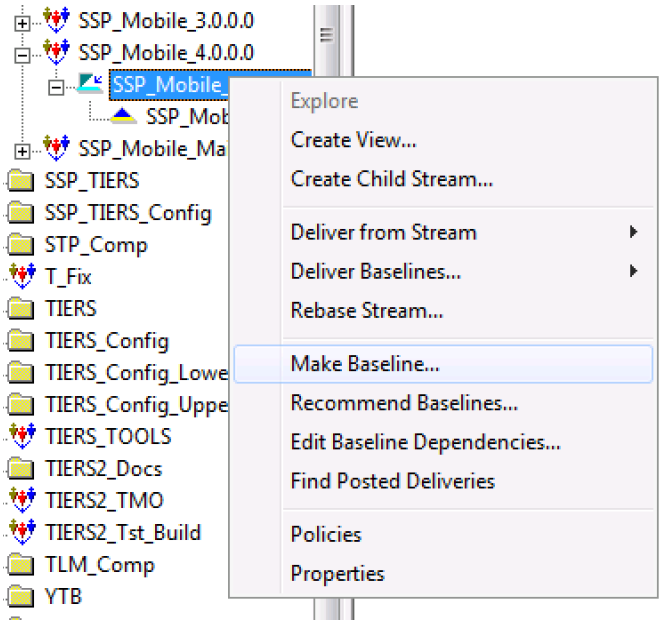


Figure 15 Create Manual Baseline

- For 'Base Name:' enter the following format: MM-DD-YYYY_SSP_Mobile_RELEASEVERSION_MILESTONE.

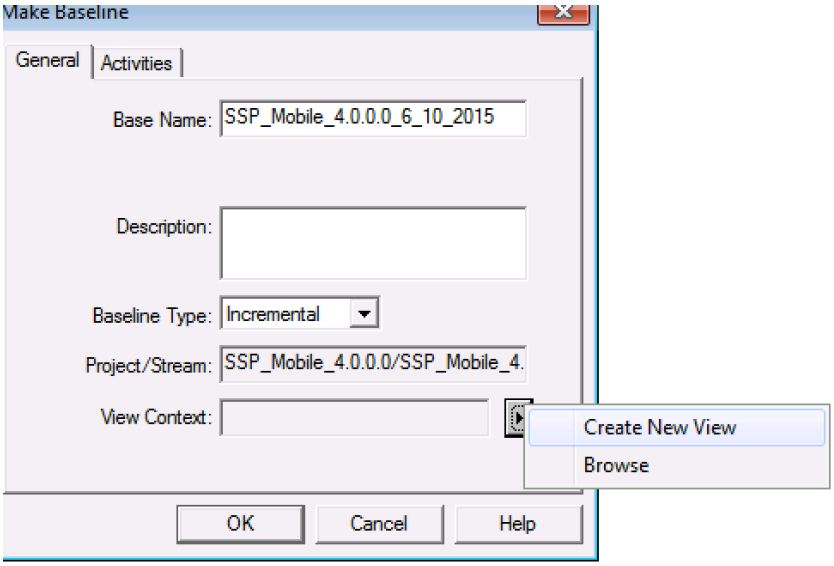


Figure 16 Naming the manual Baseline

- Select the right arrow in 'View Context:' and select browse. Then select the SSP_Mobile_VERSION_TST view. Hit 'OK.'

11 Documentation Management

Deliverables and work products are tracked by the HHSC and Deloitte PMO teams to support timely delivery, review, and response. Deliverables and work products are uploaded, versioned, managed, tracked, stored, and archived in a SharePoint site that is maintained by HHSC. Deliverables are sent to HHSC IT SSA Project Management Office who then forwards to the appropriate HHSC stakeholders for review and comment.

Attachment E:
TIERS
Data Center Services (DCS)
IS Controls

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Texas Health and Human Services Commission
Information Security and Privacy Requirements

Standards and Regulations:
Contractors are required to comply with HHSC Information Security and Privacy requirements in order to maintain a business relationship with Texas HHSC. Accordingly, contractors are required to adhere to all applicable standards and regulations (and their associated security controls) to include state laws, federal laws, executive orders, policies, regulations, standards, and guidance.

Standards and Regulations that Apply to this Contract:
Based on data types that are accessed, created, disclosed, received, transmitted, maintained, or stored within Information System(s) of this contract the following standards and regulations apply:

Texas HHSC Requirements:
The contractor is responsible for implementing the **HHS MODERATE** (NIST SP 800-53R4 MODERATE equivalent) security baseline and the **HIPAA, CMS-MARS-E,** overlays found in the IS-Controls and the following Texas HHSC standards and regulations:

- **Attachment F - HHS Information Security Controls (IS-Controls) version 1.0**
- **Attachment G - Information Security Assessment Supplemental Guidance for External Entities**
- **Exhibit D - HHSC Data Use Agreement (DUA) and Security Privacy Inquiry(SPI)**

State and Federal Requirements:
The contractor is additionally responsible for implementing the following state and federal standards and regulations:

- Texas Department of Information Resources (DIR) Security Control Standards Catalog
- Center for Medicaid & Medicare Services Minimum Acceptable Risk Security and Privacy Controls for Exchanges (CMS-MARS-E)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- NIST SP 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule
- US Department of Health and Human Services HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

Contract Monitoring:
Contractors are required to fulfill HHSC monitoring requirements for continuing compliance as outlined in the IS-RAMP.

Required Information Security & Privacy Controls that Apply to this Contract:
Table 1 below is a list of required security controls mandated by the applicable state and federal regulations listed above. The contractor is required to implement the following list of Information Security and Privacy controls unless there exists a documented agreement that establishes Texas Health and Human Services as the provider for a specified control(s).

Additionally, the contractor is required to implement any additional controls added or modified in subsequent updates to applicable standards and regulations.

If more than one applicable Standard and/or Regulation requires the same Information Security and Privacy control, then the contractor must implement the most restrictive requirements for the specified control.

Table 1: Information Security & Privacy Controls Minimum Baseline that apply to this Contract

Control ID	Control Name
AC-01	ACCESS CONTROL POLICY AND PROCEDURES
AC-02	ACCOUNT MANAGEMENT
AC-02(01)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT
AC-02(02)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS
AC-02(03)	DISABLE INACTIVE ACCOUNTS
AC-02(04)	AUTOMATED AUDIT ACTIONS
AC-02(07)	ROLE-BASED SCHEMES
AC-03	ACCESS ENFORCEMENT
AC-03(09)	CONTROLLED RELEASE
AC-04	INFORMATION FLOW ENFORCEMENT
AC-05	SEPARATION OF DUTIES
AC-06	LEAST PRIVILEGE
AC-06(01)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS
AC-06(02)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS
AC-06(05)	PRIVILEGED ACCOUNTS
AC-06(09)	AUDITING USE OF PRIVILEGED FUNCTIONS
AC-06(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS
AC-07	UNSUCCESSFUL LOGON ATTEMPTS
AC-08	SYSTEM USE NOTIFICATION
AC-10	CONCURRENT SESSION CONTROL
AC-11	SESSION LOCK
AC-11(01)	PATTERN-HIDING DISPLAYS
AC-12	SESSION TERMINATION
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
AC-16	SECURITY ATTRIBUTES
AC-17	REMOTE ACCESS
AC-17(01)	AUTOMATED MONITORING / CONTROL

Control ID	Control Name
AC-17(02)	PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION
AC-17(03)	MANAGED ACCESS CONTROL POINTS
AC-17(04)	PRIVILEGED COMMANDS / ACCESS
AC-18	WIRELESS ACCESS
AC-18(01)	AUTHENTICATION AND ENCRYPTION
AC-19	ACCESS CONTROL FOR MOBILE DEVICES
AC-19(05)	FULL DEVICE / CONTAINER-BASED ENCRYPTION
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS
AC-20(01)	LIMITS ON AUTHORIZED USE
AC-20(02)	PORTABLE STORAGE DEVICES
AC-21	INFORMATION SHARING
AC-22	PUBLICLY ACCESSIBLE CONTENT
AT-01	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
AT-02	SECURITY AWARENESS TRAINING
AT-02(02)	INSIDER THREAT
AT-03	ROLE-BASED SECURITY TRAINING
AT-04	SECURITY TRAINING RECORDS
AU-01	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
AU-02	AUDIT EVENTS
AU-02(03)	REVIEWS AND UPDATES
AU-03	CONTENT OF AUDIT RECORDS
AU-03(01)	ADDITIONAL AUDIT INFORMATION
AU-04	AUDIT STORAGE CAPACITY
AU-05	RESPONSE TO AUDIT PROCESSING FAILURES
AU-05(01)	AUDIT STORAGE CAPACITY
AU-06	AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-06(01)	PROCESS INTEGRATION
AU-06(03)	CORRELATE AUDIT REPOSITORIES
AU-07	AUDIT REDUCTION AND REPORT GENERATION
AU-07(01)	AUTOMATIC PROCESSING
AU-08	TIME STAMPS
AU-08(01)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
AU-09	PROTECTION OF AUDIT INFORMATION
AU-09(04)	ACCESS BY SUBSET OF PRIVILEGED USERS
AU-10	NON-REPUDIATION
AU-11	AUDIT RECORD RETENTION
AU-12	AUDIT GENERATION
AU-12(01)	SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL
AU-13	MONITORING FOR INFORMATION DISCLOSURE
AU-16	CROSS-ORGANIZATIONAL AUDITING
CA-01	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
CA-02	SECURITY ASSESSMENTS
CA-02(01)	INDEPENDENT ASSESSORS
CA-03	SYSTEM INTERCONNECTIONS
CA-03(05)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS
CA-05	PLAN OF ACTION AND MILESTONES
CA-05(01)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY
CA-06	SECURITY AUTHORIZATION

Control ID	Control Name
CA-07	CONTINUOUS MONITORING
CA-07(01)	INDEPENDENT ASSESSMENT
CA-08	PENETRATION TESTING
CA-09	INTERNAL SYSTEM CONNECTIONS
CM-01	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
CM-02	BASELINE CONFIGURATION
CM-02(01)	REVIEWS AND UPDATES
CM-02(03)	RETENTION OF PREVIOUS CONFIGURATIONS
CM-03	CONFIGURATION CHANGE CONTROL
CM-03(02)	TEST / VALIDATE / DOCUMENT CHANGES
CM-04	SECURITY IMPACT ANALYSIS
CM-04(01)	SEPARATE TEST ENVIRONMENTS
CM-04(02)	VERIFICATION OF SECURITY FUNCTIONS
CM-05	ACCESS RESTRICTIONS FOR CHANGE
CM-05(01)	AUTOMATED ACCESS ENFORCEMENT / AUDITING
CM-05(05)	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES
CM-06	CONFIGURATION SETTINGS
CM-06(01)	AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION
CM-07	LEAST FUNCTIONALITY
CM-07(01)	PERIODIC REVIEW
CM-07(02)	PREVENT PROGRAM EXECUTION
CM-07(04)	UNAUTHORIZED SOFTWARE / BLACKLISTING
CM-08	INFORMATION SYSTEM COMPONENT INVENTORY
CM-08(01)	UPDATES DURING INSTALLATIONS / REMOVALS
CM-08(03)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION
CM-08(05)	NO DUPLICATE ACCOUNTING OF COMPONENTS
CM-09	CONFIGURATION MANAGEMENT PLAN
CM-10	SOFTWARE USAGE RESTRICTIONS
CM-10(01)	OPEN SOURCE SOFTWARE
CM-11	USER-INSTALLED SOFTWARE
CP-01	CONTINGENCY PLANNING POLICY AND PROCEDURES
CP-02	CONTINGENCY PLAN
CP-02(01)	COORDINATE WITH RELATED PLANS
CP-02(02)	CAPACITY PLANNING
CP-02(03)	RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
CP-02(05)	CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
CP-02(08)	IDENTIFY CRITICAL ASSETS
CP-03	CONTINGENCY TRAINING
CP-04	CONTINGENCY PLAN TESTING
CP-04(01)	COORDINATE WITH RELATED PLANS
CP-06	ALTERNATE STORAGE SITE
CP-06(01)	SEPARATION FROM PRIMARY SITE
CP-06(03)	ACCESSIBILITY
CP-07	ALTERNATE PROCESSING SITE
CP-07(01)	SEPARATION FROM PRIMARY SITE
CP-07(02)	ACCESSIBILITY
CP-07(03)	PRIORITY OF SERVICE
CP-08	TELECOMMUNICATIONS SERVICES

Control ID	Control Name
CP-08(01)	PRIORITY OF SERVICE PROVISIONS
CP-08(02)	SINGLE POINTS OF FAILURE
CP-09	INFORMATION SYSTEM BACKUP
CP-09(01)	TESTING FOR RELIABILITY / INTEGRITY
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
CP-10(02)	TRANSACTION RECOVERY
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS
IA-01	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
IA-02	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-02(01)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS
IA-02(02)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS
IA-02(03)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS
IA-02(08)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT
IA-02(11)	REMOTE ACCESS - SEPARATE DEVICE
IA-03	DEVICE IDENTIFICATION AND AUTHENTICATION
IA-04	IDENTIFIER MANAGEMENT
IA-05	AUTHENTICATOR MANAGEMENT
IA-05(01)	PASSWORD-BASED AUTHENTICATION
IA-05(02)	PKI-BASED AUTHENTICATION
IA-05(03)	IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION
IA-05(07)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS
IA-05(11)	HARDWARE TOKEN-BASED AUTHENTICATION
IA-06	AUTHENTICATOR FEEDBACK
IA-07	CRYPTOGRAPHIC MODULE AUTHENTICATION
IA-08	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
IR-01	INCIDENT RESPONSE POLICY AND PROCEDURES
IR-02	INCIDENT RESPONSE TRAINING
IR-03	INCIDENT RESPONSE TESTING
IR-03(02)	COORDINATION WITH RELATED PLANS
IR-04	INCIDENT HANDLING
IR-04(01)	AUTOMATED INCIDENT HANDLING PROCESSES
IR-05	INCIDENT MONITORING
IR-06	INCIDENT REPORTING
IR-06(01)	AUTOMATED REPORTING
IR-07	INCIDENT RESPONSE ASSISTANCE
IR-07(01)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT
IR-08	INCIDENT RESPONSE PLAN
IR-09	INFORMATION SPILLAGE RESPONSE
MA-01	SYSTEM MAINTENANCE POLICY AND PROCEDURES
MA-02	CONTROLLED MAINTENANCE
MA-03	MAINTENANCE TOOLS
MA-03(01)	INSPECT TOOLS
MA-03(02)	INSPECT MEDIA
MA-03(03)	PREVENT UNAUTHORIZED REMOVAL
MA-04	NONLOCAL MAINTENANCE
MA-04(01)	AUDITING AND REVIEW
MA-04(02)	DOCUMENT NONLOCAL MAINTENANCE
MA-04(03)	COMPARABLE SECURITY / SANITIZATION

Control ID	Control Name
MA-05	MAINTENANCE PERSONNEL
MA-06	TIMELY MAINTENANCE
MP-01	MEDIA PROTECTION POLICY AND PROCEDURES
MP-02	MEDIA ACCESS
MP-03	MEDIA MARKING
MP-04	MEDIA STORAGE
MP-05	MEDIA TRANSPORT
MP-05(04)	CRYPTOGRAPHIC PROTECTION
MP-06	MEDIA SANITIZATION
MP-06(01)	REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY
MP-06(02)	EQUIPMENT TESTING
MP-07	MEDIA USE
MP-07(01)	PROHIBIT USE WITHOUT OWNER
MP-CMS-01	MEDIA RELATED RECORDS
PE-01	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
PE-02	PHYSICAL ACCESS AUTHORIZATIONS
PE-02(01)	ACCESS BY POSITION / ROLE
PE-03	PHYSICAL ACCESS CONTROL
PE-04	ACCESS CONTROL FOR TRANSMISSION MEDIUM
PE-05	ACCESS CONTROL FOR OUTPUT DEVICES
PE-06	MONITORING PHYSICAL ACCESS
PE-06(01)	INTRUSION ALARMS / SURVEILLANCE EQUIPMENT
PE-08	VISITOR ACCESS RECORDS
PE-09	POWER EQUIPMENT AND CABLING
PE-10	EMERGENCY SHUTOFF
PE-11	EMERGENCY POWER
PE-12	EMERGENCY LIGHTING
PE-13	FIRE PROTECTION
PE-13(01)	DETECTION DEVICES / SYSTEMS
PE-13(02)	SUPPRESSION DEVICES / SYSTEMS
PE-13(03)	AUTOMATIC FIRE SUPPRESSION
PE-14	TEMPERATURE AND HUMIDITY CONTROLS
PE-15	WATER DAMAGE PROTECTION
PE-16	DELIVERY AND REMOVAL
PE-17	ALTERNATE WORK SITE
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS
PE-19	INFORMATION LEAKAGE
PE-20	ASSET MONITORING AND TRACKING
PL-01	SECURITY PLANNING POLICY AND PROCEDURES
PL-02	SYSTEM SECURITY PLAN
PL-02(03)	PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
PL-04	RULES OF BEHAVIOR
PL-04(01)	SOCIAL MEDIA AND NETWORKING RESTRICTIONS
PL-08	INFORMATION SECURITY ARCHITECTURE
PS-01	PERSONNEL SECURITY POLICY AND PROCEDURES
PS-02	POSITION RISK DESIGNATION
PS-03	PERSONNEL SCREENING
PS-04	PERSONNEL TERMINATION

Control ID	Control Name
PS-05	PERSONNEL TRANSFER
PS-06	ACCESS AGREEMENTS
PS-07	THIRD-PARTY PERSONNEL SECURITY
PS-08	PERSONNEL SANCTIONS
RA-01	RISK ASSESSMENT POLICY AND PROCEDURES
RA-02	SECURITY CATEGORIZATION
RA-03	RISK ASSESSMENT
RA-05	VULNERABILITY SCANNING
RA-05(01)	UPDATE TOOL CAPABILITY
RA-05(02)	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED
RA-05(03)	BREADTH / DEPTH OF COVERAGE
RA-05(05)	PRIVILEGED ACCESS
SA-01	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
SA-02	ALLOCATION OF RESOURCES
SA-03	SYSTEM DEVELOPMENT LIFE CYCLE
SA-04	ACQUISITION PROCESS
SA-04(01)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
SA-04(02)	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS
SA-04(09)	FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE
SA-05	INFORMATION SYSTEM DOCUMENTATION
SA-08	SECURITY ENGINEERING PRINCIPLES
SA-09	EXTERNAL INFORMATION SYSTEM SERVICES
SA-09(01)	RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS
SA-09(02)	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES
SA-09(05)	PROCESSING, STORAGE, AND SERVICE LOCATION
SA-10	DEVELOPER CONFIGURATION MANAGEMENT
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION
SA-11(01)	STATIC CODE ANALYSIS
SA-11(02)	THREAT AND VULNERABILITY ANALYSES
SA-11(05)	PENETRATION TESTING
SA-11(08)	DYNAMIC CODE ANALYSIS
SA-12	SUPPLY CHAIN PROTECTION
SA-14	CRITICALITY ANALYSIS
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN
SA-22	UNSUPPORTED SYSTEM COMPONENTS
SC-01	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
SC-02	APPLICATION PARTITIONING
SC-04	INFORMATION IN SHARED RESOURCES
SC-05	DENIAL OF SERVICE PROTECTION
SC-06	RESOURCE AVAILABILITY
SC-07	BOUNDARY PROTECTION
SC-07(03)	ACCESS POINTS
SC-07(04)	EXTERNAL TELECOMMUNICATIONS SERVICES
SC-07(05)	DENY BY DEFAULT / ALLOW BY EXCEPTION
SC-07(07)	PREVENT SPLIT TUNNELING FOR REMOTE DEVICES
SC-07(08)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS
SC-07(12)	HOST-BASED PROTECTION

Control ID	Control Name
SC-07(13)	ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS
SC-07(18)	FAIL SECURE
SC-08	TRANSMISSION CONFIDENTIALITY AND INTEGRITY
SC-08(01)	CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION
SC-08(02)	PRE / POST TRANSMISSION HANDLING
SC-10	NETWORK DISCONNECT
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
SC-12(02)	SYMMETRIC KEYS
SC-13	CRYPTOGRAPHIC PROTECTION
SC-15	COLLABORATIVE COMPUTING DEVICES
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES
SC-18	MOBILE CODE
SC-19	VOICE OVER INTERNET PROTOCOL
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
SC-23	SESSION AUTHENTICITY
SC-28	PROTECTION OF INFORMATION AT REST
SC-28(01)	CRYPTOGRAPHIC PROTECTION
SC-31	COVERT CHANNEL ANALYSIS
SC-32	INFORMATION SYSTEM PARTITIONING
SC-39	PROCESS ISOLATION
SC-44	DETONATION CHAMBERS
SC-ACA-01	ELECTRONIC MAIL
SC-ACA-02	FAX USAGE
SI-01	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
SI-02	FLAW REMEDIATION
SI-02(01)	CENTRAL MANAGEMENT
SI-02(02)	AUTOMATED FLAW REMEDIATION STATUS
SI-03	MALICIOUS CODE PROTECTION
SI-03(01)	CENTRAL MANAGEMENT
SI-03(02)	AUTOMATIC UPDATES
SI-04	INFORMATION SYSTEM MONITORING
SI-04(01)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM
SI-04(02)	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS
SI-04(04)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
SI-04(05)	SYSTEM-GENERATED ALERTS
SI-04(14)	WIRELESS INTRUSION DETECTION
SI-05	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES
SI-06	SECURITY FUNCTION VERIFICATION
SI-07	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY
SI-07(01)	INTEGRITY CHECKS
SI-07(07)	INTEGRATION OF DETECTION AND RESPONSE
SI-08	SPAM PROTECTION
SI-08(01)	CENTRAL MANAGEMENT

Control ID	Control Name
SI-08(02)	AUTOMATIC UPDATES
SI-10	INFORMATION INPUT VALIDATION
SI-11	ERROR HANDLING
SI-12	INFORMATION HANDLING AND RETENTION
SI-16	MEMORY PROTECTION
PM-01	INFORMATION SECURITY PROGRAM PLAN
PM-02	SENIOR INFORMATION SECURITY OFFICER
PM-03	INFORMATION SECURITY RESOURCES
PM-04	PLAN OF ACTION AND MILESTONES PROCESS
PM-05	INFORMATION SYSTEM INVENTORY
PM-06	INFORMATION SECURITY MEASURES OF PERFORMANCE
PM-07	ENTERPRISE ARCHITECTURE
PM-08	CRITICAL INFRASTRUCTURE PLAN
PM-09	RISK MANAGEMENT STRATEGY
PM-10	SECURITY AUTHORIZATION PROCESS
PM-11	MISSION/BUSINESS PROCESS DEFINITION
PM-12	INSIDER THREAT PROGRAM
PM-13	INFORMATION SECURITY WORKFORCE
PM-14	TESTING, TRAINING, AND MONITORING
PM-15	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
PM-16	THREAT AWARENESS PROGRAM
AP-01	AUTHORITY TO COLLECT
AP-02	PURPOSE SPECIFICATION
AR-01	GOVERNANCE AND PRIVACY PROGRAM
AR-02	PRIVACY IMPACT AND RISK ASSESSMENT
AR-03	PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS
AR-04	PRIVACY MONITORING AND AUDITING
AR-05	PRIVACY AWARENESS AND TRAINING
AR-06	PRIVACY REPORTING
AR-07	PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT
AR-08	ACCOUNTING OF DISCLOSURES
DI-01	DATA QUALITY
DI-01(01)	VALIDATE PII
DI-02	DATA INTEGRITY AND DATA INTEGRITY BOARD
DI-02(01)	PUBLISH AGREEMENTS ON WEBSITES
DM-01	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION
DM-01(01)	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION
DM-02	DATA RETENTION AND DISPOSAL
DM-02(01)	SYSTEM CONFIGURATION
DM-03	MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH
DM-03(01)	RISK MINIMIZATION TECHNIQUES
IP-01	CONSENT
IP-01(01)	MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT
IP-02	INDIVIDUAL ACCESS
IP-03	REDRESS
IP-04	COMPLAINT MANAGEMENT
IP-04(01)	RESPONSE TIMES
SE-01	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Control ID	Control Name
SE-02	PRIVACY INCIDENT RESPONSE
TR-01	PRIVACY NOTICE
TR-01(01)	REAL-TIME OR LAYERED NOTICE
TR-02	SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS
TR-02(01)	PUBLIC WEBSITE PUBLICATION
TR-03	DISSEMINATION OF PRIVACY PROGRAM INFORMATION
UL-01	INTERNAL USE
UL-02	INFORMATION SHARING WITH THIRD PARTIES

Attachment F: HHS Information Security IS-Controls v1.0

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

Statement of Work (SOW)

HHS Information Security

PUBLIC

Information Security Controls (IS-Controls)

Version (v) 1.0

Formerly known as Enterprise Information Security Standards and Guidelines (EISSG and ISSG)

TEXAS
Health and Human Services

February 9, 2018

Table of Contents

Table of Contents i
1. Introduction 1
1.1. Purpose 1
1.2. Background 1
1.3. Scope 3
1.4. Target Audience 3
1.5. Alignment 3
1.6. Definitions 3
2. Security Life Cycle 4
2.1. Information System Security Categorization 4
2.2. Security Control Selection and Tailoring 11
2.3. Security Control Implementation and Documentation 12
2.4. Information System Risk and Security Assessments 13
2.5. Information System Authority to Operate 20
2.6. Monitoring Security Controls 21
3. Information Security in the Cloud 23
3.1. HHS Cloud Requirements 24
3.2. Federal Cloud Requirements 26
4. How to Use this Document 30
4.1. Control Structure 30
Appendix A: Security Baselines and Overlays 37
Appendix B: HHS Information Security Controls 65
(AC) ACCESS CONTROLS 65
(AT) AWARENESS AND TRAINING 126
(AU) AUDIT AND ACCOUNTABILITY 132
(CA) SECURITY ASSESSMENT AND AUTHORIZATION 158
(CM) CONFIGURATION MANAGEMENT 177
(CP) CONTINGENCY PLANNING 207
(IA) IDENTIFICATION AND AUTHENTICATION 231
(IR) INCIDENT RESPONSE 256
(MA) MAINTENANCE 277

(MP) MEDIA PROTECTION 288
(PE) PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS 302
(PL) PLANNING 323
(PM) PROGRAM MANAGEMENT 331
(PS) PERSONNEL SECURITY 344
(RA) RISK ASSESSMENT 356
(SA) SYSTEM AND SERVICES ACQUISITION 366
(SC) SYSTEM AND COMMUNICATIONS PROTECTION 394
(SI) SYSTEM AND INFORMATION INTEGRITY 440
Appendix C: HHS Information Security and Privacy Controls 470
(AP) AUTHORITY AND PURPOSE 470
(AR) ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT 473
(DI) DATA QUALITY AND INTEGRITY 484
(DM) DATA MINIMIZATION AND RETENTION 488
(IP) INDIVIDUAL PARTICIPATION AND REDRESS 494
(SE) SECURITY 501
(TR) TRANSPARENCY 504
(UL) USE LIMITATION 509
Appendix D: HIPAA Security Rules to IS-Controls Mapping 514
Appendix E: Security Control Risk Score Formula 520
Appendix F: References and Resources 523

Publication Information

Authorized By:	HHS Chief Information Security Officer (CISO) Shirley Erp
Supersedes:	Information Security Standards and Guidelines (EISSG/ISSG) Controls Catalog v6

Publication Version History

Numbering convention: Version. Revision as n.xx. Pre-publication drafts are 0.xx; first published version is 1.00; for minor revisions to a published document, increment the decimal number (ex. 1.01); for major content upgrades to a published document, increment the leading whole number (ex.2.00).

Revision	Date	Change Description
1.0	February 9, 2018	First published version of HHS Information Security Controls. This document fully replaces the Enterprise Information Security Standards and Guidelines (EISSG) and Information Security Standards and Guidelines (ISSG). All previous versions of those publications are rescinded and no longer valid.

Publication Review History

To satisfy the requirements of the Information Systems Security Program, a formal review of this document was conducted in accordance with HHS requirements on the following dates:

Revision	Date	Reviewer	Review Comments
1.0	February 9, 2018	Shirley Erp, Chief Information Security Officer	Authorized publication of v1

1. Introduction

Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24 Agency Information Security Program requires that all state agencies have an information security program consistent with the rules defined in the TAC 202.

The Texas Health and Human Services (HHS) Circular C-021 establishes the Information Security Program for the HHS system which is aligned with the HHS Strategic Plan for supporting the mission and functions of the HHS agencies. The HHS Information Security program is comprised of security policies, standards, controls, and guidelines. This document, IS-Controls, is an expansion of the HHS Information Security Policy (IS-Policy) requirements.

1.1. Purpose

The security and privacy controls contained in this document are the safeguards or countermeasures that, when implemented and enforced, will satisfy the information security compliance requirements defined in the HHS IS-Policy and applicable federal laws, executive orders, directives, policies, HHS regulations and standards.

1.2. Background

The HHS IS Program is based on the following three security objectives of confidentiality, integrity and availability:

Confidentiality
"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.

Integrity
"Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information.

Availability
"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of availability is the disruption of access to or use of information or an information system.

Security and privacy controls are designed to protect and meet the security objectives of confidentiality, integrity, and availability of information and the information system, reducing risk to a manageable level.

The IS-Controls supports the risk management process by specifying the minimum information security and control requirements that agencies shall use based on information system security categorization levels with the objective of reducing risk to an acceptable level.

The comprehensive set of security and privacy controls contained in the IS-Controls protects not only information and systems, but also individual employees and HHS as a whole. As such, these security and privacy controls represent the HHS organization's strong commitment to information systems security.

Certain federal programs, such as Internal Revenue Service Federal Tax Information (IRS FTI), Social Security Administration (SSA), Federal Bureau of Investigation (FBI) Criminal Justice Information (CJI), and Centers for Medicare / Medicaid Services (CMS) have specific control implementation standards that are required (See 2.1.2 for a full list of applicable federal standards.) Each Federal agency has unique data protection regulations and requirements. HHS systems and their contractors must adhere to the safeguard requirements of the Federal agencies when mandated by a contractor and interconnection agreement.

Prior to IS-Controls v1.0, there was no single, integrated, comprehensive approach to security and privacy that addressed all applicable federal requirements. These laws differ in areas of system categorization, selection of operational security controls, and the use of program management controls. Given the diversity of federal and state laws and regulations governing security and privacy that may apply, Texas HHS has amended IS-Controls to identify key standards and processes to support compliance with the current body of laws and regulations. Nothing in this document should be construed to eliminate the obligation for a HHS system or contractor to comply with the requirements of other applicable bodies of laws/regulations that apply. Depending on the information processed, a HHS information system or contractor system may be required to meet additional security control requirements as mandated by specific sources.

1.3. Scope

All HHS employees, contractors, third party users, external service providers and all HHS physical, software, and information assets (whether standalone or attached to the HHS local and wide area networks), that access, create, disclose, receive, transmit, maintain, or store HHS information, as well as all services that support or otherwise handle those physical, software, and information assets, are required to comply with the security and privacy controls contained within this document.

The security controls outlined in this document are required upon release of this document, and compliance should be documented in the information systems next annual risk assessment.

1.4. Target Audience

The IS-Controls is intended to serve a diverse audience of information systems, Information Owners, Information Custodians and Information Security staff. While all users of HHS information systems assets should be aware of security controls as adopted by HHS Information Security, primary users of this document are the information custodians of IT operations, system and database administrators, application developers, support, maintenance personnel, and Information Security Officers.

1.5. Alignment

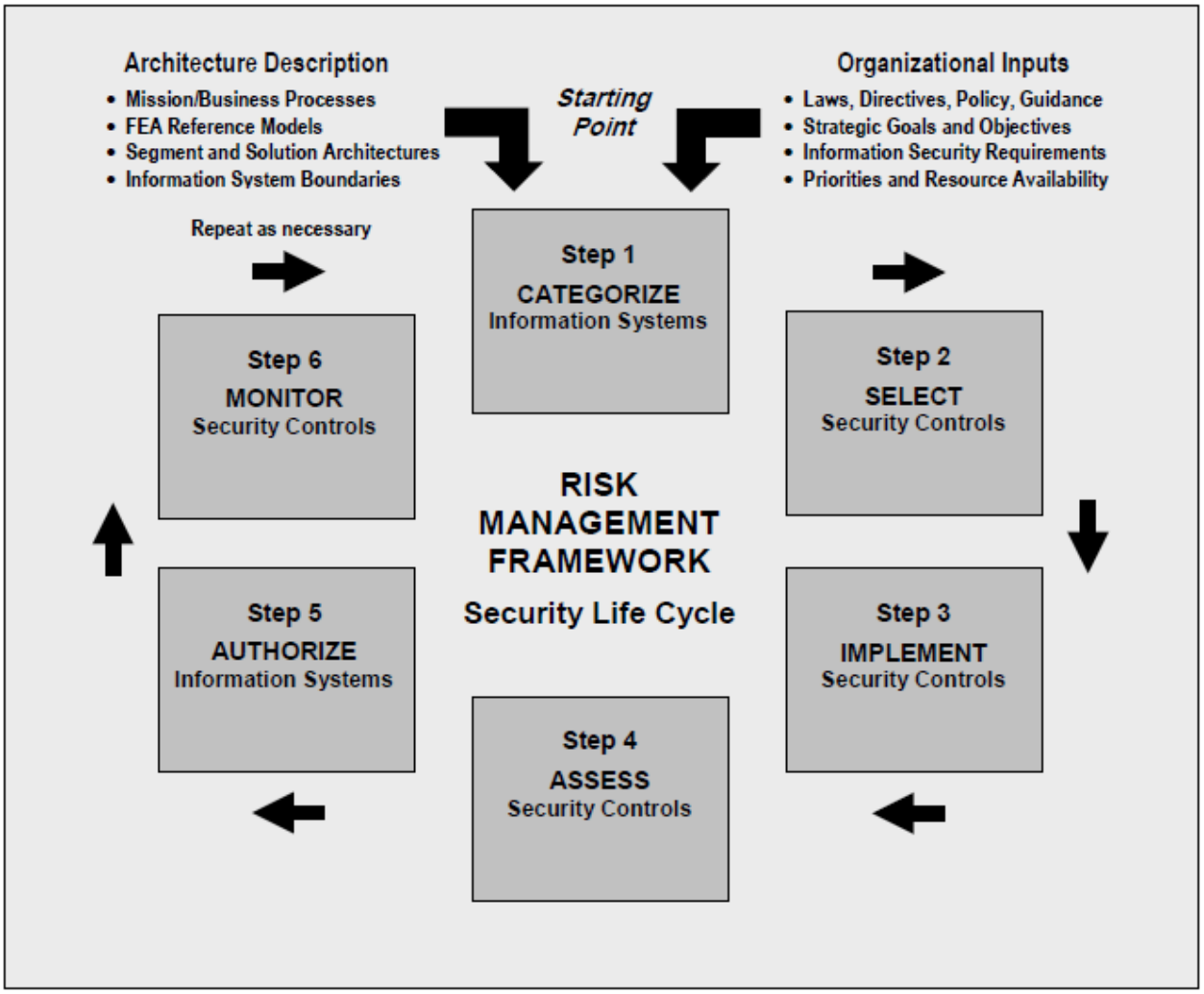
The HHS Information Security Program makes extensive use of the information security guidance found in the Department of Information Resources (DIR) Security Control Standards Catalog and the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Revision 4 (rev 4) and is based on the NIST SP 800-53 rev 4 suite of controls.

1.6. Definitions

The terms used in the IS-Controls, and other HHS Information Security documents are defined in the HHS Information Security (IS)-Definitions document.

2. Security Life Cycle

The IS-Controls specifies the minimum information security requirements that are necessary to provide the appropriate levels of information security according to risk levels. The HHS Security Life Cycle is based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). The RMF incorporates security in six steps of the security life cycle:



2.1. Information System Security Categorization

The identification and selection of the applicable baseline and overlay(s) of security controls is essential to ensure the proper controls are selected, implemented and assessed.

Security control baselines, listed in Appendix A, are the starting point for the security control selection process and are the minimum required HHS security controls a system must implement. They are chosen based on the

security category and impact of the types of data the information system processes. There are four control baselines, listed in Table 2.1 below, that are aligned with the applicable security categorization and impact levels of the data the information system processes.

Table 2.1. Security Categorization and Control Baselines

Control Baselines	Regulation Drivers	Data Classification	Security Categorization & Impact
Low	State	Public	Low
Low Plus	State	Agency Sensitive	Low
Moderate	State and Federal	Confidential	Moderate
High	State and Federal	Confidential	High

Identifying and selecting the correct baseline and overlay(s) of security controls begins with determining the security categorization level and baseline of the information system.

The following steps should be followed to determine the appropriate baselines and overlay(s) that apply.

2.1.1. Step 1: Determine Information System HHS Data Classification:

One of the core components of determining the security baseline is dependent upon the classification of data. To do this, evaluate all HHS data that is stored, processed, or maintained by the information system using the HHS Data Classification Standard. Select the highest (most confidential) data classification level and use that as the data classification for the information system.

The potential data classifications are:

- Public
- Agency Sensitive
- Confidential

2.1.2. Step 2: Determine Applicable Overlays

Overlays are additional requirements that add to or replace portions of the security control baseline. More than one overlay can be selected concurrently, and overlays exists for Texas HHS, State, and Federal requirements.

Review and select all applicable overlays that apply to the information system.

Table 2.2. Texas HHS Overlays

Overlay	Required For:
SPI	Information systems that are owned or managed by a contractor that creates, receives, maintains, uses, discloses, or has access to HHS Confidential Information and is required to sign a security and privacy inquiry (SPI). **Reference:** Information Security and Privacy Inquiry
Web & Mobile	Information systems that can be accessed through a web browser or a mobile application.
Cloud	Information systems that will reside in a non-HHS managed data center.

Table 2.3. State and Federal Overlays

Overlay	Required For:
HIPAA	Information systems that create, receive, maintain, use, disclose, or have access to Protected Health Information (PHI). **Reference:** Texas Health and Safety Code, Chapter 181; 45 C.F.R § 160.103
CMS-MARS-E	1. Information Systems that are an ACA Administering Entity[1] or contractor, subcontractor, their respective facilities supporting such IT system that access, create, disclose, receive, transmit, maintain, or store CMS data received from the CMS Federal Service Hub; 2. Or systems that interconnect (See CA-03) with the ACA Administering Entity (either directly to the Administering Entity or indirectly through an interconnection to a system that directly connects to the Administering Entity) to access, create, disclose, receive, transmit, maintain, or store CMS data.[2] Note 1: For Texas, the Texas Integrated Eligibility Redesign System (TIERS) is the primary ACA Administering Entity. "Administering Entity" means Exchanges or Marketplaces, whether federal or state, state Medicaid agencies, Children's Health Insurance Program (CHIP) agencies, or state agencies administering the Basic Health Program.

Overlay	Required For:
	Note 2: CMS Data is any data provided by CMS through their Federal Service Hub. **Reference:** Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges v2.0 (Volumes 1 - 4)
CMS-ARS	Information systems that support a Center for Medicaid and Medicare Services (CMS) business mission and perform work on behalf of CMS, has a contract with CMS or one of their contractors **that mandates CMS-ARS, and** is not required to follow CMS-MARS-E. **Reference:** CMS Acceptable Risk Safeguards v3.0
IRS	Information Systems that store, process, maintain or return information legally receive Federal Tax Information (FTI) directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. Note: FTI may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements. **Reference:** IRS Publication1075, *Tax Information Security Guidelines For Federal, State, and Local Agencies*
CJIS	Applicable to every individual contractor, private entity non-criminal justice agency representative or member of a criminal justice entity with access to, or who operates in support of criminal justice services and information. The Federal Bureau for Investigation (FBI) Criminal Justice Information System (CJIS) provides data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

Overlay	Required For:
	1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data. 2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual. 3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case. 4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII). 5. Case/Incident History—information about the history of criminal incidents. **References:** https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
VA	Applies to all VA Information Systems, contractor operated services and information resources located and operated at contract facilities or any other third party utilizing VA information or VA information systems in order to perform a VA authorized activity. **References:** Veteran's Affairs Handbook 6500, *Risk Management Framework for VA Information Systems*
SSA	Information under the control of SSA that is provided to an external entity under the terms of an information exchange agreement with SSA. However, "SSA data/information" also includes information provided to the Electronic Information Exchange Partners (EIEP) by a source other than SSA, but which the EIEP attests to that SSA verified it, or the EIEP couples the information with data from SSA as to certify the accuracy of the information. **Reference:**

Overlay	Required For:
	Contact HHS Information Security if access is needed to the SSA overlay.
FERPA	Applies to an educational agency or institution that receives funds under one or more of the programs covered by the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA is a Federal law that protects the privacy of student education records. *Educational agency or institution* is any public or private agency or institution. *Education program* means any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, adult education, and any program that is administered by an educational agency or institution. **References:** https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Select Agent	Information Systems subject to select agent regulations in 42 C.F.R that is managed jointly by the Center for Disease Control (CDC) and United States Department of Agriculture (USDA). The Select Agent Program oversees the possession, use, and transfer of biological select agents and toxins which have the potential to pose a severe threat to public, animal or plant health, or animal or plant products. **References:** Select Agency Information System Security Controls Guidance
NCHHSTP	Information systems subject to the CDC Data Security and Confidentiality guidelines for HIV, Viral Hepatitis, Sexually Transmitted Diseases, and Tuberculosis Programs (NCHHSTP). This applies to all systems funded by NCHHSTP or for systems that receive data from a system funded by NCHHSTP. **References:** NCHHSTP

2.1.3. Step 3: Determine Initial Security Baseline

Once the information system data classification and overlays have been determined, the initial security baseline can be calculated. Use the following table to determine the correct security control baseline:

Table 2.4. Data Classification to Security Baseline

Data Classification	Has an Applicable Federal Overlay	Security Control Baseline Is:
Public		Low
Agency Sensitive		Low Plus
Confidential	No	Moderate
Confidential	Yes	Proceed to Table 2.5

If the information system has a confidential data classification and any applicable State or Federal overlays, the following additional questions must be answered to determine if the High or Moderate security control baseline is applicable.

Table 2.5. Confidential Federal Systems Security Control Baseline

Categorization Questions:	Security Control Baseline Is:
Information system is directly involved in making payments for Medicare Fee-for-Service (FFS) or Medicaid and State Children's Health Insurance Program **AND** the CMS-ARS overlay is applicable.	High
If the above is not applicable:	Moderate

2.1.4. Step 4: Finalize Security Baseline

The security control baseline (Step 3), when combined with the applicable overlays (Step 2), determine the minimum required security controls for the Information System. Any control, in Appendix A, with an (x) in the applicable baseline or overlays is required and should be included in the Information Systems baseline. The final security baseline and applicable overlays should be documented in the system security plan (SSP).

Increasing the Security Control Baseline Requirements

The Information Owner, if they determine that the security control baseline is not sufficient to protect the information system, may either:

1. Increase the security control baseline to a higher level (e.g., moderate to high), or

2. Select individual controls from a higher baseline to add to the security control requirements. See 2.2, Security Control Selection and Tailoring for further information on adding additional controls to compensate for risk.

All decisions to modify the security control baseline must be documented, along with justification concerning the reason why, in the SSP.

2.2. Security Control Selection and Tailoring

Control selection is the process of tailoring the initial list of required security controls (based on the security baseline and overlay(s)). The Information Owner, working with the systems Information Custodian(s), uses the tailoring process to modify and appropriately align the controls more closely with the specific conditions with the organization. All control selection and tailoring decisions must be documented in the SSP.

The tailoring process includes:

a. Identifying Inheritable (Common) Controls: Identifying and designating controls as "inherited" common controls are the controls that the information system inherits from organizational common control providers. HHS Information Security maintains the list of inheritable common controls for HHS information systems. Contractors that access, create, disclose, receive, transmit, maintain, or store HHS information must coordinate with HHS to determine the common controls that they may inherit, if any, from HHS.

b. Identifying Partially Inheritable (Hybrid) Controls: Identifying security controls that are partially inherited from organizational common control providers and are also partially provided by the information system. These controls are known as "hybrid" controls and HHS Information Security maintain the list of security controls inheritable as *hybrid* for HHS Information systems. Contractors that access, create, disclose, receive, transmit, maintain, or store HHS information must coordinate with HHS to determine hybrid controls they inherit from HHS.

c. Identifying Not Applicable Controls: Identifying security controls that are "*Not Applicable*" to the information system. This does not include removing security controls for operational convenience. A decision to mark a control as "Not Applicable" must be defensible based on the specific rationale and the decision must be documented in the SSP. Common reasons for marking a security control as "*Not Applicable"* include:

1. *Technology related considerations*: Security controls that refer to specific technologies (e.g., wireless, cryptography, public key

infrastructure) are applicable only if those technologies are employed or are required to be employed.

2. *Single User Systems*: For information systems that are designed to operate as single-user systems (e.g., smart phones), several of the security controls that address sharing among users may not be needed. Security controls such as AC-10, Concurrent Session Control, SC-4, Information in Shared Resources, and AC-3, Access Enforcement may not be required in single-user systems/operations.
3. *Mobility*: If those information systems operate primarily in mobile environments (e.g., mobile phones), the security control baseline should be tailored appropriately to account for the differences in mobility and accessibility of the specific locations where the systems reside. For example, many of the security controls in the Physical and Environmental Protection (PE) family that are selected in all three baselines reflect the assumption that the information systems reside in physical facilities/complexes that require appropriate physical protections.
4. *Data Connectivity and Bandwidth*: While many information systems are interconnected, there are some systems which for security or operational reasons, lack networking capabilities—that is, the systems are air gapped from the network. For non-networked systems, security controls such as AC-17, *Remote Access*, SC-8, *Transmission Confidentiality and Integrity*, and SC-7, *Boundary Protection*, are not applicable and may be tailored out of the security control baselines.

d. System-Specific Controls: All controls that are not identified as “common” or “hybrid” are considered system specific and must be fully implemented solely by the information system.

e. Identifying Compensating Controls: If the initial baseline of controls is not sufficient to mitigate the risk to the system, the Information Owner may identify and add other security controls not included in the initial list of required security controls in order to compensate for unresolved risk. The reasoning and justification for adding security controls to the initial list must be clearly documented in the SSP.

2.3. Security Control Implementation and Documentation

Once the information system’s required security controls have been finalized, the controls should be implemented by the information system and how they are implemented documented in the applicable SSP.

2.3.1. Security Control Implementation

Early integration of information security requirements into the system development life cycle is the most cost-effective method for implementing the organizational risk management strategy.

All portions of applicable security control requirements and implementation standards are required to be implemented by the information system or a common control provider unless a security exception is approved using the methodology document in Section 2.4.3 or the control has been determined to be "Not Applicable."

2.3.2. Documenting Information System Security

Security control documentation describes how system-specific, hybrid, and common controls are implemented. The system security plan (SSP) serves as the primary method to document how security controls are implemented (including planned inputs, expected behavior, and expected outputs). Contact HHS Information Security for the current version of the SSP.

The SSP documents the following information (at a minimum) about the information system:

a. Description: The description is an overview of the information system that includes identifying the purpose of the information system, information owner, custodians, categorization, security baselines, location, and data flows.

b. Environment and Boundaries: The system environment and boundaries include describing the architecture, topology, and system boundary; all system hardware and software assets; the used ports, protocols, and services; and all of the user community authorized to use the system.

c. Security Control Implementation: The implementation section is used to document how each applicable security control is implemented and its current implementation status.

2.4. Information System Risk and Security Assessments

2.4.1. Risk Assessments

The information owner is required by TAC 202 to conduct a risk assessment of their information system prior to receiving its first Authorization to Operate (ATO) (section 2.5) and on an annual basis.

As defined in RA-03, this risk assessment will include:

a. A review of the compliance status of all security and privacy controls required per the system categorization.

b. Documenting the current implementation status of required security controls in the system security plan (SSP), to include creating findings for any security controls identified as not being fully in place.

c. A review of all security documents including the system categorization, SSP, contingency plans, and any open findings.

d. A vulnerability assessment of the information system to detect if the system is vulnerable to unauthorized access or harm, including the extent to which the systems electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

The results of the risk assessment should be sent to the Information Security Officer for review. This report is due prior to requesting the system undergoing a security assessment, and subsequently no-later-than the Information Systems ATO anniversary date each year.

2.4.2. Security Assessments

Security assessments are conducted, if required, by the Information Security Office or an authorized third party provider after a risk assessment has been completed, and are used to determine the extent to which the information system's security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security Assessments are conducted on information systems when determined as required by the Authorizing Official (see section 2.5). The output of a security assessment is a Security Assessment Report (SAR).

Security assessments can require a significant amount of organizational resources to conduct. Due to that, the Chief Information Security Officer, working with the Authorizing Official, must determine the level of effort required for each security assessment using a risk-based approach. Security assessment level-of-effort can be classified by defining the assessment methods, depth, and coverage that will be used.

a. Security Assessment Methods: The Information Security Office can leverage a wide variety of methods when conducting security assessments. The methods selected are dependent upon the criticality of the system and the level of effort required to conduct the assessment, and not all assessment methods are required to be used in every security assessment.

Assessment methods include:

1. Examine: This is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (e.g., system security plans, product specifications, security controls, etc.). The purpose of this method is to facilitate the security assessor's understanding of the information system, clarification of an aspect of the system, or obtaining evidence.
2. Interview: This method is the process of holding discussions with individuals or groups of individuals to facilitate the security assessor's understanding, achieve clarification, or obtain evidence.
3. Test: This method is the process of exercising one or more assessment objects (e.g., vulnerability scans, configuration scans, penetration tests, etc.).

b. Assessment Depth and Coverage: Prior to starting each security assessment, the expected depth and coverage of the assessment must be identified and documented by Information Security. The two attributes, depth and coverage, are critical to define the level of effort and timeframe for the assessment.

1. Depth: This attribute addresses the rigor and level of detail in the security assessment methods that will be used in the assessment process.
2. Coverage: This attribute addresses the scope or breadth of the assessment, including number and types of items to examine or test and number of people to interview.

Both attributes are broken into three categories: basic, focused, and comprehensive. For each attribute and method, a decision must be made and documented using Table 2.6 and Table 2.7 below as to the level of effort that will be spent by security assessors. See NIST 800-53A Appendix D for further information.

c. Scenarios

The following scenarios are examples, and not official standards. Contact the Information Security Office for the current methodology used to determine the assessment depth and coverage for security assessment of HHS Information Systems.

Scenario 1 - Public system, internal only:
This system is deemed to pose a very low risk to the organization. Due to this, the Information Security Office selects the following level of effort:

- Depth: Examine (Basic)

- Coverage: Examine (Basic)

Scenario 2 - Internet facing system that transmits HHS confidential data:
This system is required to have a full security assessment and penetration test conducted due to Texas Government Code 2054.516. Due to that, the Information Security Office selects the following levels:

- Depth: Examine (Focused), Interview (Focused), Test (Comprehensive)
- Coverage: Examine (Comprehensive), Interview (Focused), Test (Focused)

Table 2.6: Depth Assessment Attribute Categories by Method

	Basic	Focused	Comprehensive
Examine	High level reviews, checks, observations, or inspections	A more in-depth study/analysis of the system. Requires a substantial body of evidence or documentation.	An in-depth, detailed, and thorough study/analysis of the controls. Requires an extensive body of evidence or documentation.
Interview	Broad-based high level discussion with individuals and groups	More in-depth discussion in specific areas with individuals or groups	Probing discussions in specific areas with individuals or groups of individuals
Test	Black box testing: Assumes no knowledge of the internal structure and implementation details	Gray box testing: Assumes some knowledge of the internal structure and implementation details	White box testing: Assumes explicit and substantial knowledge of the internal structure and implementation details

Table 2.7: Coverage Assessment Attribute Categories by Method

	Basic	Focused	Comprehensive
Examine	A representative sample of security controls and other assessment objects	A larger sample of security controls deemed particularly important to achieving the objective	A sufficiently large sample, or all, required security controls
Interview	Representative sample of individuals in key organizational roles	Representative sample of individuals in key organizational roles and specific individuals deemed particularly important to achieving assessment objectives	Large sample of individuals in key organizational roles and specific individuals deemed particularly important to achieving assessment objectives
Test	Representative sample of assessment objects	Representative sample of assessment objects and other assessment objects deemed particularly important	Sufficiently large sample of assessment objects

2.4.3. Remediation

Remediation begins after a weakness has been documented as a finding by Information Security, and is the process of identify how to resolve the weaknesses and deficiencies identified in the information system. This process begins with the Information Owner and Custodian analyzing the identified weakness or deficiency and determining the methodology to resolve the finding. This decision, called the initial risk decision, should be made within the below time frames of receiving notification of a validated finding.

Finding Criticality	Days to Make Risk Decision
Low Risk Findings	90 Days
Moderate Risk Findings	60 Days
High Risk Findings	30 Days

There are two generally accepted methods for resolving findings: remediate (e.g., correct) the weakness; or receive authorization to accept the risk (e.g., do not correct) from a senior agency official with the authority to accept the risk (see 2.4.3.c).

a. Risk Levels: Weaknesses are assigned a Risk Level by Information Security based on the severity.

- High Risk (High Impact): Risk that could cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- High Risk: Risk to an information resource's confidentiality, integrity, or availability that could be expected to have a severe adverse effect on organizational operations, organizational assets, or individuals but not meet the requirement for high impact risk.
- Moderate Risk: Risk to an information resource's confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- Low Risk: Risk to an information resource's confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

b. Risk Remediation: After weaknesses have been identified and a finding issued, a remediation strategy must be developed. This should be a collaborative effort with stakeholders including the Information Owner, Information Custodian, System Developers and Maintainers, Information Security Officers, CISO, and others as needed.

Depending on the risk level of the weakness, reasonable timeframes are granted for remediation:

- High Risk: 90 business days from the date the risk decision is due
- Moderate Risk: 180 business days from the date the risk decision is due
- Low Risk: 365 business days from the date the risk decision is due

Plan of Action and Milestone (POA&M): A POA&M is a formal documented plan for how the weakness will be remediated. A POA&M should clearly explain how the identified weakness will be corrected, including required steps, estimated timelines, who will complete the work, and costs.

When writing a POA&M to remediate a weakness, the organization should consider several factors:

- *Required Work*: Remediation plans often require multiple steps in order to be completed. These are documented as milestones, which include estimated delivery dates, resource requirements, and a description of what the milestone will accomplish.
- *Compensating Controls*: Identify any controls already in place or that could be put in place that would adequately reduce the risk posed the weakness to an acceptable level.
- *Funding Requirements*: The remediation process requires resources; the type and amount of which will vary. Estimation of resources required should be done carefully, with consideration to:
    - The complexity of the corrective action plan
    - Parties required to execute the corrective action plan
    - Purchasing requirements

Prioritization: Resource limitations often prevent the stakeholders from obtaining the necessary resources to mitigate every identified weakness within the same time period. The careful prioritization of weakness helps ensure that critical important weaknesses are appropriately rank-ordered and allocated resources required to resolve the associated risk. Prioritization efforts should consider:

- *Risk Level/Severity*: Sensitivity and criticality of information on the system; the estimated likelihood of the weakness occurring and/or being exploited; the cost of a potential occurrence/exploitation in terms of dollars, man-hours, and/or reputation.
- *Analysis*: The weakness must be analyzed to determine if there are any other processes or system relationships that it may affect.
- *Resources*: Some weaknesses can be quickly and easily resolved without a large expenditure of time or money. In those cases, weaknesses may be addressed ahead of those weakness for which resourcing must be planned and budgeted.
- *Management Input*: Senior management and/or authorizing officials should have input into prioritizing remediation.
- *Other Weaknesses*: A combination of minor, overlapping weaknesses may highlight a more serious problem.
- *Breadth*: Whether the weakness is a systemic issue or an isolated event.
- *Source*: Whether the weakness identified through a method, such as an audit, which demands greater attention.
- *Visibility*: In some cases a lower level weakness is a higher priority due to it garnering external visibility.

c. Risk Acceptance: In rare cases, the Information Owner can present a case for accepting, transferring, or mitigating risk instead of remediating the risk. In these instances, the risk exception process should be initiated by the Information Owner. Risk exceptions are not permanent and must be reviewed and reauthorized (normally once a year).

Table 2.8. Risk Exceptions Authorized Approvers

Security / Impact Risk Rating	Information Owner	ISO	CISO	CIO	Agency Head
Low Security Risk	Approve	Approve			
Moderate Security Risk	Approve	Approve			
High Security Risk [1]	Approve	Coordinate	Approve		
High Impact Risk [2]	Approve	Coordinate	Coordinate	Coordinate	Approve

[1] High Security Risk is risk that, per the HHS Security Control Risk Score Formula or the ISO, has been determined to be high risk and requires CISO approval. The HHS CISO is responsible for deciding whether the High Security Risk meets the criteria for "High Impact Risk."

[2] High Impact Risk, Per TAC 202, could cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage

to organizational assets; result in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

2.5. Information System Authority to Operate

An Authorization to Operate (ATO) is a formal declaration by a senior organizational official that authorizes operation of an Information System and explicitly accepts the risk to agency operations. The ATO is signed after the system has undergone a risk assessment that validates that the system has met and passed all requirements to become operational.

CA-06, *Security Authorization*, per the DIR Security Control Standards Catalog, mandated by Texas Administrative Code 202.26, requires that a senior organizational official accepts any residual risk and authorizes information systems for processing before the system begins operations or anytime it undergoes a significant change. This official is referred to as the Authorizing Official. The Authorizing Official, by granting an information system an ATO, formally accepts responsibility for the residual risk the information system poses to the organization. The Authorizing Official cannot delegate their responsibilities to other officials within the organization.

2.5.1. Security Authorization Package

The Authorizing Official, in order to make a well informed risk-based authorization decision requires an authorization package that is comprised of several key documents. These documents, when combined, provide the minimum necessary documentation required for the Authorizing Official to determine whether the risk posed by the system is acceptable.

The authorization package, prepared by the Information Owner and/or Custodian, at a minimum, includes:

a. System Security Plan (SSP): This document, outlined in section 2.3 and PL-02, provides a comprehensive overview of the information system and its current security posture.

b. Security Assessment Report (SAR): This document, described in section 2.4.2 and CA-02, is a formal report that documents the results of a risk assessment, and if requested, security assessment, and any weaknesses or deficiencies identified during the assessment(s).

c. Finding Plans of Action and Milestones (POA&M): These documents, described in section 2.4.3 and CA-05, document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the Information System's security controls and to reduce or eliminate known vulnerabilities in the system.

2.5.2. Risk Determination and Acceptance

The explicit acceptance of risk is the responsibility of the Authorizing Official and cannot be delegated to other officials within the organization. The Authorizing Official, in collaboration with the Chief Information Security Officer, considers many factors when deciding if the risk to organization operations (including mission, function, image, or reputation), organizational assets, individuals, other organization, and the State, is acceptable. Security authorization decisions are based on the content of the security authorization package (section 2.5.1) and, where appropriate, any input from key organization officials.

The Authorizing Official formally documents their decision in an authorization decision document. This document must contain the following information:

a. Authorization decision: Indicates whether the Information System is (a) Authorized to Operate or (b) Not Authorized to Operate

b. Terms and Conditions for the Authorization: Provides a description of any specific limitations or restrictions placed on the operation of the information system.

c. Authorization Termination Date: Indicates when the authorization termination date expires. This is normally set at three years, as documented in CA-06, but can be set to a more restrictive timeframe.

The authorization decision document, once complete, is delivered to the Information Owner and Chief Information Security Officer and becomes a formal component of the information system's security documentation.

2.6. Monitoring Security Controls

After the information system is authorized to operate, the security controls in the information system must be monitored on an ongoing basis. This includes documenting changes to the system or its environment of operation and conducting security impact analyses of the associated changes, conducting annual risk assessments, and reporting the security state of the system to designated organizational officials.

2.6.1. Changes to the Information System and its Environment of Operations

Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the system resides and operates. Anytime the information system is modified or changed, a security impact analysis (SIA) (CM-04) should be conducted by the Information Owner and/or Custodian to

determine the extent to which the proposed or actual changes to the information system or its environment of operation may affect the security controls currently in place. The results of the SIA determines if the change is a:

a. Routine Change: This change is handled through the organizations continuous monitoring strategies documented in section 2.6.2 and section 2.6.3. This does not impact the system's current ATO.

b. Minor Change: This change requires a reassessment of affected information security controls, normally referred to as a security evaluation. This does not impact the system's current ATO, however the results of the security evaluation must be considered before the change is approved for operation by the Change Control Board (CCB). Additionally, any weaknesses identified in the security evaluation must be tracked as findings against the information system if the change is approved.

c. Significant Change: This change is of a significant enough nature that the system will require a full security assessment and a new ATO before the updated system may be moved to an operational environment.

2.6.2. Ongoing Risk Assessments

Subsequent to the initial authorization, the information owner is required by TAC 202 to conduct a risk assessment of their information system on a bi-annual basis. See section 2.4.1 for further information.

2.6.3. Ongoing Remediation Actions

Receiving an Authority to Operate does not relieve the Information Owner of the responsibility to remediate risks identified in the Security Assessment Report or through other means after the ATO is granted. Findings, unless granted an exception, must be remediated within the timeframes established by the organization.

3. Information Security in the Cloud

As defined by NIST, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

This cloud model promotes availability and is composed of five essential characteristics, three service model, and four deployment models."

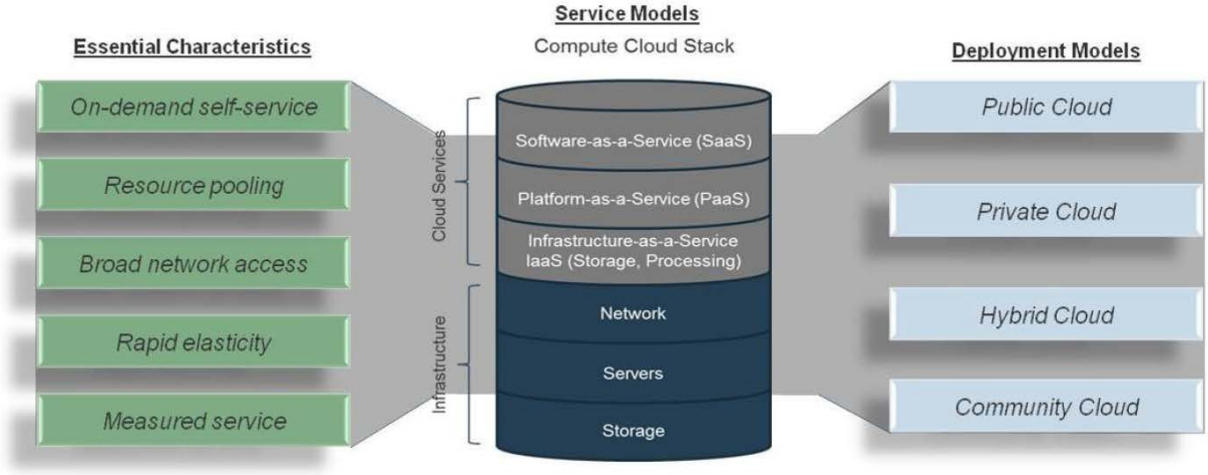
While cloud computing offers many potential benefits, it is not without risk. The primary security concerns with cloud computing are:

- Data is not stored in an agency-managed data center
- The agency must rely on the provider's security controls for protection
- Data is not transferred securely between the cloud provider and service consumer
- Interfaces to access data in a cloud environment, including authentication and authorization controls, may not be secured per customer requirements
- Data from multiple customers is potentially commingled in the cloud environment

An agency's cloud implementation is a combination of a service model and a deployment model. Service models consist of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Deployment models consist of private, community, public, and hybrid clouds.

[1] Advanced Internet-Based Computing Service as defined in §2157.007(a), Texas Government Code can be used synonymously with the term cloud computing

Cloud Computing Characteristics, Service Models, and Deployment Models [2]



The risk to data varies in each of the four deployment models, with private cloud typically being the lowest risk model and public cloud being the highest risk model. Depending on the deployment model, compensating controls can be accepted in place of the mandatory requirements, but those compensating controls must provide the same level of protection as mandatory controls.

The service and deployment model used in a cloud computing environment will determine the responsibility for security controls implementation between the agency and the cloud provider for the protection of data that is stored or processed in the cloud environment.

3.1. HHS Cloud Requirements

3.1.1. All HHS Information Systems using Cloud Services

a. The Cloud Service Provider (CSP) must agree to comply with all applicable security controls outlined in this publication.

b. All use of cloud service providers must be approved using the HHS IT governance process, to include approval by the HHS CISO, prior to being deployed to the cloud environment and must comply with all TGC 2054.391 requirements.[3]

[2] Source: Texas Cloud Services, Guide for State Agencies and Institutions of Higher Education

[3] DIR, in its capacity as manager of the Data Center Services (DCS) program, has determined that the use of Software as a Service (SaaS) as a managed service is consistent with the state strategic plan and the DCS framework; however, if an agency is contemplating a SaaS solution outside the DCS program, an approved exemption is required. See http://dir.texas.gov/View-Contracts-And-Services/Pages/Content.aspx?id=34 for more information.

c. The use of cloud services to store, process, or maintain HHS Agency Sensitive or HHS Confidential data requires the establishment of a HHS contractual agreement between the cloud service provider and HHS.

3.1.2. HHS Information Systems using Cloud Services to Store, Process, or Maintain Confidential Information

For any HHS Confidential data that is received, processed, stored, or transmitted in a cloud environment, the cloud service provider will not offshore HHS confidential data unless all of the following requirements are met:

- The information system owner has received the express prior written consent from the HHS Authorizing Official.
- The data is encrypted with a FIPS 140-2 compliant[4] encryption that complies with SC-13 and SC-28.
- The offshore provider does not have access to the encryption keys.
- The information system owner maintains the encryption keys within the United States.

3.1.3. Federal Risk and Authorization Management Program (FedRAMP)

HHS Information Systems that leverage a cloud solution should consider FedRAMP authorized cloud systems.[5]

FedRAMP is a federal program that provides a standardized approach to security assessments, authorizations, and continuous monitoring for cloud products and services. The FedRAMP program, based on NIST 800-53, provides assurance that FedRAMP authorized cloud systems have undergone an assessment by a Third Party Assessment Organization (3PAO) and have been authorized as meeting minimum security requirements as defined in the FedRAMP impact levels.

The following table should be used when considering which FedRAMP authorized cloud system to utilize:

HHS Security Control Baseline	FedRAMP Impact Level
Low	Low
Low Plus	Moderate

[4] Some Federal Overlays require FIPS 140-2 **validated/certified** encryption versus compliant encryption

[5] The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. See https://www.fedramp.gov/ for more information.

Moderate	Moderate
High	High

If a FedRAMP authorized cloud system is leveraged, the 3PAO security assessment report can be leveraged as evidence of a completed risk assessment and security assessment for the security controls that the CSP is providing to HHS Information Systems. If a non-FedRAMP authorized cloud system is utilized, the information owner must ensure the cloud system has undergone a security assessment to validate that the CSP is compliant with HHS security requirements.

3.2. Federal Cloud Requirements

Depending on the type of data that the HHS Information System receives, processes, stores, or transmits, additional Federal cloud requirements may apply. These requirements may add additional requirements beyond what is validated by a FedRAMP 3PAO.

3.2.1. Health Insurance Portability and Accountability Act (HIPAA)

When a covered entity engages the services of a cloud service provider (CSP) to create, receive, maintain, or transmit electronic protected health information (ePHI) on its behalf, the CSP is a business associate under HIPAA. Further, when a business associate subcontracts with a cloud service provider to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the cloud service provider processes or stores only encrypted ePHI and lacks an encryption key for the data.[6]

As a business associate, the CSP must comply with the applicable standards and implementation specifications of the Security Rule with respect to ePHI. However, in cases where a CSP is providing only no-view services to a covered entity (or business associate) customer, certain Security Rule requirements that apply to the ePHI maintained by the CSP may be satisfied by both parties through the action of one of the parties.

For more information see the US Health and Human Services guidance on HIPAA & Cloud Computing located at https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

[6] Source: Guidance on HIPAA & Cloud Computing, US Health and Human Services

3.2.2. Internal Revenue Service's (IRS) Federal Tax Information (FTI)

To use a cloud computing model to receive, process, store, or transmit FTI, the agency must be in compliance with all requirements in this publication and IRS 1075. The following mandatory requirements are in effect for introducing FTI to a cloud environment:

a. Notification Requirement: The agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment (Note: advanced approval is not required, only advanced notification.)

b. Data Isolation: Software, data, and services that receive, process, store, or transmit FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

c. Service-Level Agreement (SLA): The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with its third-party cloud provider.

d. Data Encryption in Transit: FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 validated, and operate using the FIPS 140-2 validated module. This requirement must be included in the SLA.

e. Data Encryption at Rest: FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 validated and operate using the FIPS 140-2 validated module. This requirement must be included in the SLA, if applicable.

f. Persistence of Data in Relieved Assets: Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by the National Security Agency (NSA) and Central Security Service (CSS). This requirement must be included in the SLA.

g. Risk Assessment: The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing, or transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The Office of

Safeguards will evaluate the risk assessment as part of the notification requirement in Requirement (a).

h. Security Control Implementation: Customer-defined security controls must be identified, documented, and implemented. The customer-defined security controls, as implemented, must comply with requirements in this publication.

3.2.3. Federal Bureau for Investigation (FBI) Criminal Justice Information (CJI)

Receiving, processing, storing, or transmitting CJI data in a cloud environment requires full compliance with FBI CJIS Security Policy 5.6. Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren't new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

Prior to engaging in outsourcing of any criminal justice or non-criminal justice administrative functions that include CJI, the Information System Owner must:

a. Request and receive written prior permission from the DPS/CJIS System Officer (CSO) or FBI CJIS System Officer.
b. Provide the DPS/CSO copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

Contact the Texas Department of Public Safety (DPS) for current requirements for leveraging a cloud service provider to receive, process, store, or transmit CJI data on behalf of Texas HHS.

3.2.4. Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its Electronic Information Exchange Partners (EIEPs). EIEPs must protect the information with efficient and effective security controls. EIEPs are entities that have electronic information exchange agreements with the agency.

EIEPs (e.g., State Agency) cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer.

If the EIEP will store SSA-provided information through a cloud service provider (CSP), the Agency must provide to the SSA the name and address of the cloud provider and describe the security responsibilities the contract requires to protect SSA-provided information. Additionally, the State Agency, contractor(s), and agent(s) must:

a. Exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

b. Agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

c. Thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s).

3.2.5. Center for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)

CMS does not prohibit the use of external service providers. However, the following requirements must be met prior to external service providers being utilized.

a. The Agency must notify CMS of plans to outsource information systems services prior to the awarding of contract.

b. The Agency must notify CMS at least 45 days prior to transmitting data into an external information service environment.

c. The outsourcing of information system services outside of the continental U.S. must be authorized by the CIO of CMS.

For further information see the CMS-MARS-E publication series.

4. How to Use this Document

4.1. Control Structure

Each security and privacy control contains the following sections and appearance:

CONTROL ID: CONTROL NAME

Priority:	
Baseline(s):	Overlay(s):
CONTROL REQUIREMENTS	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
ASSESSMENT METHODS AND OBJECTS	

4.1.1 Control Family Numbering

The information security and privacy controls have a well-defined organization and structure. They are organized into 26 control families for ease of use in the security control selection and specification process. The families are established by NIST SP 800-53 and are in alignment with the 18 security-related, and 8 privacy families.

Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each of the 18 security control families and 8 privacy control families.

Table 4.1 Security and Privacy Control Families

Control Identifier	Control Family
Security Controls	
(AC)	Access Controls
(AT)	Awareness and Training
(AU)	Audit and Accountability
(CA)	Security Assessment and Authorization
(CM)	Configuration Management
(CP)	Contingency Planning
(IA)	Identification and Authentication
(IR)	Incident Response

(MA)	Maintenance
(MP)	Media Protection
(PE)	Physical and Environmental Protection
(PL)	Planning
(PM)	Program Management
(PS)	Personnel Security
(RA)	Risk Assessment
(SA)	System and Services Acquisition
(SC)	System and Communications Protection
(SI)	System and Information Integrity
Security and Privacy Controls	
(AP)	Authority and Purpose
(AR)	Accountability, Audit, and Risk Management
(DI)	Data Quality and Integrity
(DM)	Data Minimization and Retention
(IP)	Individual Participation and Redress
(SE)	Security
(TR)	Transparency
(UL)	Use Limitation

4.1.2. Control Overview

The HHS information security and privacy control structure consists of the Baseline/Enhancement section, Implementation Standards section, Guidance section, References section, Related Requirements section and Assessment Procedures section.

The HHS-tailored information security and privacy controls serve as the starting point for HHS Information Owners in determining the appropriate controls and countermeasures necessary to protect their information systems.

The term *organization* is utilized throughout the control requirements and associated elements. NIST SP 800-53 defines an *organization* as: "*…an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).*" HHS extends and clarifies this to include applicable supporting organizations (that is, "*…operational elements*")—including contractor organizations.

When directing and assigning minimum roles and responsibilities within control requirements, text may refer to organizational leaders such as the *CIO*. For the purposes of control requirements, understanding of these terms are to be interpreted as follows:

- For roles preceded by the term HHS, such as …*approved by the HHS CIO*…; these roles and responsibilities are to be interpreted to refer to the HHS agency official that holds that role or title. In this case, the *CIO for the Texas Health and Human Services*.

- For roles not preceded by the term HHS, such as …*approved by the CIO*…; these roles and responsibilities are to be interpreted to refer to the local official that holds that equivalent role or title. In the case of a contractor organization, the CIO might refer to a corporate *Chief Information Officer, Chief Technology Officer, or Director of Information Technology for Medicare Programs*; whatever corporate/organizational role is the equivalent of the "Chief Information Officer" within the applicable organizational structure and scope. Within the HHS government organizational structure, CIO will always refer to the HHS CIO.

4.1.3. Control ID and Name

In accordance with NIST SP 800-53, controls are divided into Baseline controls and Enhancements.

Baseline Control

The *Baseline* control is the concise statement specifying the capability needed to protect a particular aspect of the HHS information or information system at the applicable system security level.

Baseline controls are identified by security control Family ID and convey CMS policy, which are based on minimum federal requirements, and employ, and correlate directly to, NIST SP 800-53 numbering (e.g., AC-01, AC-02, AC-03…).

Baseline Enhancements

Enhancements supplement baseline controls to achieve the overall required level of protection in accordance with the system security level. Enhancements may only be required for higher system security level baselines, but may be used to strengthen the level of protection provided in lower system security level systems if deemed appropriate by the Business Owner.

Enhancement controls are structured the same as the baseline controls. Enhancement controls follow the same security control Family ID and correlate directly to NIST SP 800-53 (e.g., AC-2(1), AC-2(2), AC-2(3)…).

4.1.4. Priority

The priority value listed on the right side of the Control or Enhancement title provides the recommended priority codes used for sequencing decisions during security control implementation. Organizations can use the priority code designation associated with each security control to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control, a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control, and a Priority Code 0 [P0] indicates the security control is not selected (or has been withdrawn) for any baseline). This recommended sequencing prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the SSP have been implemented. The priority codes are intended only for implementation sequencing, not for making security control selection decisions.

4.1.5. Baseline and Overlays

Baselines and Overlays list the applicable Security Baselines and overlays that were determined during Information System Security Categorization. See Table 2.4 and Table 2.5 for a list of possible baselines and Table 2.2 and Table 2.4 for a list of possible State and Federal overlays.

4.1.6. Control Requirements

Control requirements are a concise statement specifying the capability needed to protect a particular aspect of the HHS information or information system at the applicable system security level.

If overlays are required, they are listed as a bold statement (e.g., **IRS**, **CMS-ARS**, **CMS-MARS**) followed by the overlay requirements. Overlays are only listed when they are more restrictive then the HHS requirements, and are applied using the following methodology:

a. Overlay that replaces a portion or all of the HHS requirement
If the overlay lists the same letter or number as the core requirement, then the overlay replaces the corresponding HHS requirement.

In the below example, systems that must include the CMS-MARS-E overlay would follow the more restrictive CMS-MARS-E requirement instead of the HHS requirement.

AC-12: SESSION TERMINATION

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system automatically terminates a user session after thirty (30) minutes of inactivity. **CMS-MARS-E:** The information system automatically terminates a user session after fifteen (15) minutes of inactivity	

b. Overlay that adds to the core requirement

If the overlay lists a new requirement (e.g., a new letter or number), then the requirement is in addition to the HHS requirement.

In the below example, systems that must include the CMS-ARS overlay would follow the HHS requirements, a and b, as well as the CMS-ARS requirement, c.

AT-04: SECURITY TRAINING RECORDS

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization: a. Documents and monitors individual information system security and privacy training activities, including basic security and privacy awareness training and specific role-based information system security and privacy training; and b. Retains individual training records for a minimum of five (5) years after completing a specific training course. **CMS-ARS:** c. Identifies employees and contractors who hold the roles with significant information security and privacy responsibilities	

c. No additional overlay requirement listed:

If the control lists a required overlay but no additional overlay requirements are listed, then the HHS control requirements fully implements all overlay (e.g., State or Federal) requirements.

d. Multiple Conflicting Overlay(s):

If the information system has been categorized as having more than one required overlay, and the overlay requirements conflict, always implement the most restrictive (e.g., secure) of the overlay requirements.

In the example below, CMS-ARS requires high systems to disable identifiers after 30 days of inactivity, and CMS-MARS-E to disable identifiers after 60 days of inactivity. In this example, the most restrictive requirement is 30 days, which should be selected.

IA-04: IDENTIFIER MANAGEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization manages information system identifiers by: e. Disabling the identifier after ninety (90) days of inactivity **CMS-ARS:** e. Disabling the identifier after the following period of in activity: 30 days for High, 60 days for Moderate, or 90 days for Low and Low Plus systems. **CMS-MARS-E:** e. The organization manages information system identifiers by disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process.	

4.1.7. Implementation Standards

The purpose of the implementation standard is to provide additional implementation requirements for the associated security control.

Implementation standards contain specific HHS and/or overlay definitions or event values (such as “90 days”) to be implemented as the compliance standard for a given control. All implementation standards must be implemented at the designated system security level and for applicable “Overlays” for all information and information systems that store, process, or maintain HHS data.

Overlays in implementation standards follow the same rules as described in section 4.1.6.

4.1.8. Supplemental Guidance

The control may include additional guidance to explain the intent of the control. In some cases, these include specific HHS or Overlay requirements or recommendations. Otherwise, the section refers to NIST and other federal publications for further guidance. It is a recommended security practice to refer to the guidance and procedures for additional information to have a clearer and more detailed understanding of specifics of the requirement to assist the organization meeting the HHS security requirements.

4.1.9. References

The references section identifies the Texas HHS, State, and/or Federal source documents which are the basis for the applicable control requirements.

4.1.10. Related Control

Many, but not all, controls may be related to one or more other controls. When addressing some controls, it may be important that their

implementation documentation during an assessment or audit be consistent with one or more related controls. At the very least, organizations must take care to ensure that related control implementations do not conflict. While every effort was made to identify related controls, other unidentified relationships may exist that are unique to a particular system, contract type, or organization. Related controls also serve as potential compensating controls and should be used accordingly.

4.1.11. Assessment Procedures

The Assessment Procedures, including Assessment Objectives, and Assessment Methods and Objects, help determine if the security control implementations in the information system are effective (i.e., implemented correctly, operating as intended, and producing the desired outcome). They provide a foundation to support the security assessment and authorization process. The "Assessment Procedure" section consists of two sub-sections that are designated to achieve one or more objectives by applying methods to assessment objects.

Assessment Objectives

The "Assessment Objectives" include a set of determination statements ("Determine if…") related to the particular control under assessment. The determination statements are closely linked to the content of the control (i.e., the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements.

The assessment expectations provide assessors with important reference points for the level of assurance (i.e., grounds for confidence) needed for the determination of security control effectiveness. Each of the Assessment Objective determination statements is either traceable to requirements within the baseline or enhancement security control. This ensures that all aspects of the security control are fully assessed and that any weaknesses or deficiencies in the control can be identified and corrective actions taken (usually in the form of a POA&M).

Assessment Methods and Objects

The assessment methods provide a recommended assessment action for evaluators to test the control such as *Examine*, *Interview*, and *Test*. The satisfactory/non-satisfactory result(s) ascertained by the evaluation of the security control provides an understanding of the effective implementation of the control. A Risk Posture may be obtained, and/or Risk Based Decisions can be made by combining multiple control evaluation results together.

Appendix A: Security Baselines and Overlays

The SSA overlay is available upon request from the HHS Information Security Office.

The Cloud, VA, FDA, Threat Agent, and NCHHSTP overlays will be added in a future edition of IS-Controls. See the federal control documents listed in section 2.1.2 for details concerning overlay control requirements.

CMS-ARS control requirements vary depending on the types of data and the type of system on which it resides (e.g., Cloud, PII, PHI). See the CMS-ARSv3.0 publication for the specific CMS-ARS control baselines that will apply to the information system.

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
AC-01	**ACCESS CONTROL POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AC-02	**ACCOUNT MANAGEMENT**	P1	X	X	X	X	X			TAC 202.22(1)(B)	X	X	X	X	X	X	X	X
AC-02(01)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT	P1			X	X							X	X		X	X	
AC-02(02)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	P1			X	X							X	X			X	
AC-02(03)	DISABLE INACTIVE ACCOUNTS	P1			X	X							X	X		X	X	
AC-02(04)	AUTOMATED AUDIT ACTIONS	P1			X	X							X	X		X		
AC-02(05)	INACTIVITY LOGOUT	P1				X							X					
AC-02(07)	ROLE-BASED SCHEMES	P1											X	X		X		
AC-02(09)	RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS	P1											X					
AC-02(10)	SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION	P1											X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
AC-02(11)	USAGE CONDITIONS	P1				X							X					
AC-02(12)	ACCOUNT MONITORING / ATYPICAL USAGE	P1				X							X					
AC-02(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	P1				X							X					
AC-03	**ACCESS ENFORCEMENT**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AC-03(03)	MANDATORY ACCESS CONTROL	P0														X		
AC-03(04)	DISCRETIONARY ACCESS CONTROL	P0														X		
AC-03(09)	CONTROLLED RELEASE	P1											X	X				
AC-04	**INFORMATION FLOW ENFORCEMENT**	P1		X	X	X					X	X	X	X	X	X	X	X
AC-04(08)	SECURITY POLICY FILTERS	P1																
AC-04(12)	DATA TYPE IDENTIFIERS	P1											X					
AC-04(15)	DETECTION OF UNSANCTIONED INFORMATION	P1											X					
AC-04(17)	DOMAIN AUTHENTICATION	P1											X					
AC-04(18)	SECURITY ATTRIBUTE BINDING	P1											X					
AC-04(21)	PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS	P1											X					
AC-05	**SEPARATION OF DUTIES**	P1		X	X	X					X	X	X	X	X	X	X	
AC-06	**LEAST PRIVILEGE**	P1		X	X	X		X			X	X	X	X	X	X	X	X
AC-06(01)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS	P1			X	X							X	X	X	X	X	
AC-06(02)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	P1			X	X							X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
AC-06(03)	NETWORK ACCESS TO PRIVILEGED COMMANDS	P1				X							X					
AC-06(05)	PRIVILEGED ACCOUNTS	P1			X	X							X	X	X	X	X	
AC-06(07)	REVIEW OF USER PRIVILEGES	P1											X					
AC-06(09)	AUDITING USE OF PRIVILEGED FUNCTIONS	P1			X	X							X	X	X	X	X	
AC-06(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	P1			X	X							X	X	X		X	
AC-07	**UNSUCCESSFUL LOGON ATTEMPTS**	P2	X	X	X	X	X				X		X	X	X	X	X	X
AC-07(02)	PURGE / WIPE MOBILE DEVICE	P0													X			
AC-08	**SYSTEM USE NOTIFICATION**	P1	X	X	X	X					X		X	X	X	X	X	
AC-09	**PREVIOUS LOGON (ACCESS) NOTIFICATION**	P3				X							X			X		
AC-09(01)	UNSUCCESSFUL LOGONS	P3				X							X					
AC-10	**CONCURRENT SESSION CONTROL**	P3				X					X		X	X		X		
AC-11	**SESSION LOCK**	P3		X	X	X	X				X	X	X	X	X	X	X	X
AC-11(01)	PATTERN-HIDING DISPLAYS	P3			X	X							X	X		X	X	
AC-12	**SESSION TERMINATION**	P2		X	X	X		X			X	X	X	X	X		X	X
AC-12(01)	USER-INITIATED LOGOUTS / MESSAGE DISPLAYS	P0														X		
AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**	P3	X	X	X	X					X		X	X	X		X	
AC-16	**SECURITY ATTRIBUTES**	P1				X						X	X					
AC-16(03)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM	P1											X					
AC-17	**REMOTE ACCESS**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
AC-17(01)	AUTOMATED MONITORING / CONTROL	P1			X	X							X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
AC-17(02)	PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	P1			X	X	X						X	X	X	X	X	
AC-17(03)	MANAGED ACCESS CONTROL POINTS	P1			X	X							X	X	X	X	X	
AC-17(04)	PRIVILEGED COMMANDS / ACCESS	P1			X	X							X	X	X	X	X	
AC-17(06)	PROTECTION OF INFORMATION	P0														X		
AC-17(09)	DISCONNECT / DISABLE ACCESS	P1				X							X					
AC-18	**WIRELESS ACCESS**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
AC-18(01)	AUTHENTICATION AND ENCRYPTION	P1			X	X	X						X	X	X	X	X	
AC-18(04)	RESTRICT CONFIGURATIONS BY USERS	P1				X							X					
AC-18(05)	ANTENNAS / TRANSMISSION POWER LEVELS	P1				X							X			X		
AC-19	**ACCESS CONTROL FOR MOBILE DEVICES**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AC-19(05)	FULL DEVICE / CONTAINER-BASED ENCRYPTION	P1			X	X							X	X	X	X	X	
AC-20	**USE OF EXTERNAL INFORMATION SYSTEMS**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AC-20(01)	LIMITS ON AUTHORIZED USE	P1			X	X							X	X		X	X	
AC-20(02)	PORTABLE STORAGE DEVICES	P1			X	X							X	X	X	X	X	
AC-20(03)	NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES	P1													X			
AC-21	**INFORMATION SHARING**	P2			X	X					X	X	X	X	X	X	X	
AC-22	**PUBLICLY ACCESSIBLE CONTENT**	P3	X	X	X	X					X		X	X	X	X	X	
AC-23	**DATA MINING PROTECTION**	P0														X		X
AT-01	**SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**	P1	X	X	X	X				TAC 202.20(4)	X	X	X	X	X	X	X	X

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
AT-02	**SECURITY AWARENESS TRAINING**	P1	X	X	X	X	X			TAC 202.24(b)(2-3); TGC 2054.134(d)	X	X	X	X	X	X	X	X
AT-02(02)	INSIDER THREAT	P1			X	X							X	X	X	X	X	
AT-03	**ROLE-BASED SECURITY TRAINING**	P1	X	X	X	X				TAC 202.20(4); TAC 202.21(b)(4)	X	X	X	X	X	X	X	X
AT-04	**SECURITY TRAINING RECORDS**	P3	X	X	X	X					X	X	X	X	X	X	X	X
AU-01	**AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X		X	
AU-02	**AUDIT EVENTS**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AU-02(03)	REVIEWS AND UPDATES	P1			X	X							X	X	X	X	X	
AU-03	**CONTENT OF AUDIT RECORDS**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AU-03(01)	ADDITIONAL AUDIT INFORMATION	P1			X	X							X	X	X	X	X	
AU-03(02)	CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	P1				X							X					
AU-04	**AUDIT STORAGE CAPACITY**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AU-05	**RESPONSE TO AUDIT PROCESSING FAILURES**	P1	X	X	X	X					X		X	X	X	X	X	X
AU-05(01)	AUDIT STORAGE CAPACITY	P1				X							X	X	X	X		
AU-05(02)	REAL-TIME ALERTS	P1				X							X			X		
AU-06	**AUDIT REVIEW, ANALYSIS, AND REPORTING**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
AU-06(01)	PROCESS INTEGRATION	P1			X	X							X	X		X	X	
AU-06(03)	CORRELATE AUDIT REPOSITORIES	P1			X	X							X	X		X	X	
AU-06(05)	INTEGRATION / SCANNING AND MONITORING CAPABILITIES	P1				X							X					
AU-06(06)	CORRELATION WITH PHYSICAL MONITORING	P1				X							X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
AU-06(10)	AUDIT LEVEL ADJUSTMENT	P1																
AU-07	**AUDIT REDUCTION AND REPORT GENERATION**	P2		X	X	X					X	X	X	X	X	X	X	X
AU-07(01)	AUTOMATIC PROCESSING	P2			X	X							X	X			X	
AU-07(02)	AUTOMATIC SORT AND SEARCH	P1											X					
AU-08	**TIME STAMPS**	P1	X	X	X	X					X		X	X	X	X	X	X
AU-08(01)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	P1			X	X							X	X		X	X	
AU-09	**PROTECTION OF AUDIT INFORMATION**	P1	X	X	X	X					X		X	X	X	X	X	X
AU-09(02)	AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS	P1				X							X			X		
AU-09(03)	CRYPTOGRAPHIC PROTECTION	P1				X							X					
AU-09(04)	ACCESS BY SUBSET OF PRIVILEGED USERS	P1			X	X							X	X		X	X	
AU-10	**NON-REPUDIATION**	P2				X					X		X	X				X
AU-10(01)	ASSOCIATION OF IDENTITIES	P1											X					
AU-11	**AUDIT RECORD RETENTION**	P3	X	X	X	X					X		X	X	X	X	X	X
AU-12	**AUDIT GENERATION**	P1	X	X	X	X					X	X	X	X	X	X	X	X
AU-12(01)	SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL	P1				X							X	X				
AU-12(03)	CHANGES BY AUTHORIZED INDIVIDUALS	P1				X							X					
AU-13	**MONITORING FOR INFORMATION DISCLOSURE**											X						X
AU-16	**CROSS-ORGANIZATIONAL AUDITING**	P0												X	X			
AU-16(02)	SHARING OF AUDIT INFORMATION	P1											X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
CA-01	**SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X		X	
CA-02	**SECURITY ASSESSMENTS**	P2	X	X	X	X		X		TAC 2054.515	X	X	X	X	X	X	X	X
CA-02(01)	INDEPENDENT ASSESSORS	P2			X	X							X	X		X	X	
CA-02(02)	SPECIALIZED ASSESSMENTS	P2				X							X					
CA-02(03)	EXTERNAL ORGANIZATIONS	P2				X							X					
CA-03	**SYSTEM INTERCONNECTIONS**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CA-03(01)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	P0														X		
CA-03(02)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	P0														X		
CA-03(03)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	P1											X					
CA-03(05)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	P1			X	X							X	X	X	X	X	
CA-05	**PLAN OF ACTION AND MILESTONES**	P3	X	X	X	X				TAC 202.24(a)(5)	X		X	X	X	X	X	X
CA-05(01)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY	P3	X	X	X	X							X	X				
CA-06	**SECURITY AUTHORIZATION**	P3	X	X	X	X				TAC 202.20(6); TAC 202.25(4)	X	X	X	X	X	X	X	X
CA-07	**CONTINUOUS MONITORING**	P3	X	X	X	X					X	X	X	X	X	X	X	X
CA-07(01)	INDEPENDENT ASSESSMENT	P2			X	X							X	X		X	X	
CA-08	**PENETRATION TESTING**	P2			X	X		X		TGC 2054.516	X	X	X					X
CA-08(01)	INDEPENDENT PENETRATION AGENT OR TEAM	P2				X							X					
CA-09	**INTERNAL SYSTEM CONNECTIONS**	P2	X	X	X	X					X	X	X	X		X	X	X
CA-09(01)	SECURITY COMPLIANCE CHECKS	P1											X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
CM-01	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**	P1	X	X	X	X					X		X	X	X	X	X	
CM-02	**BASELINE CONFIGURATION**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CM-02(01)	REVIEWS AND UPDATES	P1			X	X							X	X	X	X	X	
CM-02(02)	AUTOMATION SUPPORT FOR ACCURACY / CURRENCY	P1				X							X					
CM-02(03)	RETENTION OF PREVIOUS CONFIGURATIONS	P1			X	X							X	X		X	X	
CM-02(06)	DEVELOPMENT AND TEST ENVIRONMENTS	P1				X							X					
CM-02(07)	CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS	P1				X							X			X	X	
CM-03	**CONFIGURATION CHANGE CONTROL**	P1		X	X	X					X	X	X	X	X	X	X	X
CM-03(01)	AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES	P1				X							X			X		
CM-03(02)	TEST / VALIDATE / DOCUMENT CHANGES	P1			X	X							X	X	X	X	X	
CM-03(04)	SECURITY REPRESENTATIVE	P0														X		
CM-03(06)	CRYPTOGRAPHY MANAGEMENT	P1											X					
CM-04	**SECURITY IMPACT ANALYSIS**	P2	X	X	X	X					X	X	X	X	X	X	X	
CM-04(01)	SEPARATE TEST ENVIRONMENTS	P2			X	X							X	X		X		
CM-04(02)	VERIFICATION OF SECURITY FUNCTIONS	P2				X							X			X		
CM-05	**ACCESS RESTRICTIONS FOR CHANGE**	P1		X	X	X					X	X	X	X	X	X	X	X
CM-05(01)	AUTOMATED ACCESS ENFORCEMENT / AUDITING	P1				X							X	X		X		
CM-05(02)	REVIEW SYSTEM CHANGES	P1				X							X			X		

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
CM-05(03)	SIGNED COMPONENTS	P1				X							X					
CM-05(05)	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	P1											X	X		X		
CM-05(06)	LIMIT LIBRARY PRIVILEGES	P0														X		
CM-06	**CONFIGURATION SETTINGS**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
CM-06(01)	AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION	P1				X							X	X				
CM-06(02)	RESPOND TO UNAUTHORIZED CHANGES	P1				X							X					
CM-07	**LEAST FUNCTIONALITY**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
CM-07(01)	PERIODIC REVIEW	P1			X	X							X	X		X	X	
CM-07(02)	PREVENT PROGRAM EXECUTION	P1			X	X							X	X		X	X	
CM-07(03)	REGISTRATION COMPLIANCE	P0														X		
CM-07(04)	UNAUTHORIZED SOFTWARE / BLACKLISTING	P1	X	X										X		X	X	
CM-07(05)	AUTHORIZED SOFTWARE / WHITELISTING	P1			X	X							X			X		
CM-08	**INFORMATION SYSTEM COMPONENT INVENTORY**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CM-08(01)	UPDATES DURING INSTALLATIONS / REMOVALS	P1			X	X							X	X	X	X	X	
CM-08(02)	AUTOMATED MAINTENANCE	P1				X							X					
CM-08(03)	AUTOMATED UNAUTHORIZED COMPONENT DETECTION	P1			X	X							X	X		X	X	
CM-08(04)	ACCOUNTABILITY INFORMATION	P1				X							X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
CM-08(05)	NO DUPLICATE ACCOUNTING OF COMPONENTS	P1			X	X							X	X			X	
CM-09	**CONFIGURATION MANAGEMENT PLAN**	P1		X	X	X					X	X	X	X	X	X	X	X
CM-10	**SOFTWARE USAGE RESTRICTIONS**	P2	X	X	X	X					X	X	X	X	X	X	X	X
CM-10(01)	OPEN SOURCE SOFTWARE	P2											X	X	X			
CM-11	**USER-INSTALLED SOFTWARE**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CP-01	**CONTINGENCY PLANNING POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	
CP-02	**CONTINGENCY PLAN**	P1	X	X	X	X					X	X	X	X	X		X	
CP-02(01)	COORDINATE WITH RELATED PLANS	P1			X	X							X	X		X	X	
CP-02(02)	CAPACITY PLANNING	P1				X							X	X				
CP-02(03)	RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS	P1			X	X							X	X		X	X	
CP-02(04)	RESUME ALL MISSIONS / BUSINESS FUNCTIONS	P1				X							X					
CP-02(05)	CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS	P1			X	X							X					
CP-02(08)	IDENTIFY CRITICAL ASSETS	P1			X	X							X	X		X	X	
CP-03	**CONTINGENCY TRAINING**	P2	X	X	X	X					X	X	X	X	X		X	
CP-03(01)	SIMULATED EVENTS	P2				X							X					
CP-04	**CONTINGENCY PLAN TESTING**	P2	X	X	X	X					X	X	X	X	X		X	
CP-04(01)	COORDINATE WITH RELATED PLANS	P2			X	X							X	X			X	
CP-04(02)	ALTERNATE PROCESSING SITE	P2				X							X					
CP-04(04)	FULL RECOVERY / RECONSTITUTION	P2				X							X					
CP-06	**ALTERNATE STORAGE SITE**	P1		X	X	X					X	X	X	X	X	X	X	
CP-06(01)	SEPARATION FROM PRIMARY SITE	P1			X	X							X	X		X	X	
CP-06(02)	RECOVERY TIME / POINT OBJECTIVES	P1				X							X					
CP-06(03)	ACCESSIBILITY	P1			X	X							X	X		X	X	
CP-07	**ALTERNATE PROCESSING SITE**	P1			X	X					X	X	X	X	X	X	X	
CP-07(01)	SEPARATION FROM PRIMARY SITE	P1			X	X							X	X			X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
CP-07(02)	ACCESSIBILITY	P1			X	X							X	X			X	
CP-07(03)	PRIORITY OF SERVICE	P1			X	X							X	X			X	
CP-07(04)	PREPARATION FOR USE	P1				X							X					
CP-08	**TELECOMMUNICATIONS SERVICES**	P1		X	X	X					X	X	X	X			X	
CP-08(01)	PRIORITY OF SERVICE PROVISIONS	P1			X	X							X	X			X	
CP-08(02)	SINGLE POINTS OF FAILURE	P1			X	X							X	X			X	
CP-08(03)	SEPARATION OF PRIMARY / ALTERNATE PROVIDERS	P1				X							X					
CP-08(04)	PROVIDER CONTINGENCY PLAN	P1				X							X					
CP-09	**INFORMATION SYSTEM BACKUP**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CP-09(01)	TESTING FOR RELIABILITY / INTEGRITY	P1			X	X							X	X			X	
CP-09(02)	TEST RESTORATION USING SAMPLING	P1				X							X					
CP-09(03)	SEPARATE STORAGE FOR CRITICAL INFORMATION	P1				X							X					
CP-09(05)	TRANSFER TO ALTERNATE STORAGE SITE	P1				X							X					
CP-10	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**	P1	X	X	X	X					X	X	X	X	X	X	X	X
CP-10(02)	TRANSACTION RECOVERY	P1			X	X							X	X		X	X	
CP-10(04)	RESTORE WITHIN TIME PERIOD	P1				X							X					
CP-11	**ALTERNATE COMMUNICATIONS PROTOCOLS**											X						
IA-01	**IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**	P1	X	X	X	X					X		X	X	X	X	X	
IA-02	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
IA-02(01)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS	P1			X	X							X	X	X	X	X	
IA-02(02)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	P1				X							X	X	X	X	X	
IA-02(03)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	P1				X							X	X		X	X	
IA-02(04)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	P1				X							X			X		
IA-02(05)	GROUP AUTHENTICATION	P1											X			X		

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
IA-02(06)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE	P1				X							X					
IA-02(07)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE	P1				X							X					
IA-02(08)	NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT	P1			X	X							X	X		X	X	
IA-02(09)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT	P1				X							X			X		
IA-02(11)	REMOTE ACCESS - SEPARATE DEVICE	P1			X	X							X	X	X	X	X	
IA-02(12)	ACCEPTANCE OF PIV CREDENTIALS	P1				X							X			X	X	
IA-02(13)	OUT-OF-BAND AUTHENTICATION	P0														X		
IA-03	**DEVICE IDENTIFICATION AND AUTHENTICATION**	P1		X	X	X					X	X	X	X	X	X	X	X
IA-03(01)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	P0														X		
IA-03(04)	DEVICE ATTESTATION	P0														X		
IA-04	**IDENTIFIER MANAGEMENT**	P1	X	X	X	X					X	X	X	X	X	X	X	X
IA-04(02)	SUPERVISOR AUTHORIZATION	P0														X		
IA-04(03)	MULTIPLE FORMS OF CERTIFICATION	P1																
IA-04(04)	IDENTIFY USER STATUS	P1											X			X		
IA-05	**AUTHENTICATOR MANAGEMENT**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
IA-05(01)	PASSWORD-BASED AUTHENTICATION	P1	X	X	X	X	X	X			X		X	X	X	X	X	
IA-05(02)	PKI-BASED AUTHENTICATION	P1			X	X							X	X		X	X	
IA-05(03)	IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION	P1			X	X							X	X		X	X	
IA-05(04)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION	P1											X					
IA-05(05)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY	P0														X		
IA-05(06)	PROTECTION OF AUTHENTICATORS	P1											X			X		
IA-05(07)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	P1						X					X	X		X		
IA-05(08)	MULTIPLE INFORMATION SYSTEM ACCOUNTS	P0														X		

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
IA-05(11)	HARDWARE TOKEN-BASED AUTHENTICATION	P1			X	X							X	X		X	X	
IA-06	**AUTHENTICATOR FEEDBACK**	P2	X	X	X	X					X	X	X	X	X	X	X	
IA-07	**CRYPTOGRAPHIC MODULE AUTHENTICATION**	P1	X	X	X	X					X	X	X	X	X	X	X	
IA-08	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**	P1	X	X	X	X					X		X	X	X	X	X	
IA-08(01)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	P1				X							X			X	X	
IA-08(02)	ACCEPTANCE OF THIRD-PARTY CREDENTIALS	P1				X							X			X	X	
IA-08(03)	USE OF FICAM-APPROVED PRODUCTS	P1				X							X			X	X	
IA-08(04)	USE OF FICAM-ISSUED PROFILES	P1				X							X				X	
IR-01	**INCIDENT RESPONSE POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	X
IR-02	**INCIDENT RESPONSE TRAINING**	P2	X	X	X	X					X	X	X	X	X	X	X	X
IR-02(01)	SIMULATED EVENTS	P2				X							X					
IR-02(02)	AUTOMATED TRAINING ENVIRONMENTS	P2				X							X					
IR-03	**INCIDENT RESPONSE TESTING**	P2		X	X	X					X	X	X	X	X	X	X	X
IR-03(01)	AUTOMATED TESTING	P2				X							X					
IR-03(02)	COORDINATION WITH RELATED PLANS	P2			X	X							X	X			X	
IR-04	**INCIDENT HANDLING**	P1	X	X	X	X					X	X	X	X	X	X	X	X
IR-04(01)	AUTOMATED INCIDENT HANDLING PROCESSES	P1			X	X							X	X		X	X	
IR-04(03)	CONTINUITY OF OPERATIONS	P1				X							X			X		
IR-04(04)	INFORMATION CORRELATION	P1				X							X			X		
IR-04(06)	INSIDER THREATS - SPECIFIC CAPABILITIES	P1				X							X					
IR-04(07)	INSIDER THREATS - INTRA-ORGANIZATION COORDINATION	P1				X							X					
IR-05	**INCIDENT MONITORING**	P1	X	X	X	X					X	X	X	X	X	X	X	X
IR-05(01)	AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS	P1				X							X					
IR-06	**INCIDENT REPORTING**	P1	X	X	X	X				TAC 202.23(b); TGC 2054.1125;	X	X	X	X	X	X	X	X
IR-06(01)	AUTOMATED REPORTING	P1			X	X							X	X		X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
IR-06(02)	VULNERABILITIES RELATED TO INCIDENTS	P0														X		
IR-07	**INCIDENT RESPONSE ASSISTANCE**	P3	X	X	X	X					X	X	X	X	X	X	X	X
IR-07(01)	AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT	P2			X	X							X	X		X	X	
IR-07(02)	COORDINATION WITH EXTERNAL PROVIDERS	P2											X			X		
IR-08	**INCIDENT RESPONSE PLAN**	P1	X	X	X	X					X	X	X	X	X	X	X	X
IR-09	**INFORMATION SPILLAGE RESPONSE**	P1											X	X	X	X		X
IR-09(01)	RESPONSIBLE PERSONNEL	P2											X					
IR-09(02)	TRAINING	P2											X					
IR-09(03)	POST-SPILL OPERATIONS	P2											X					
IR-09(04)	EXPOSURE TO UNAUTHORIZED PERSONNEL	P2											X					
IR-10	**INTEGRATED INFORMATION SECURITY ANALYSIS TEAM**	P2																X
MA-01	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	
MA-02	**CONTROLLED MAINTENANCE**	P2	X	X	X	X					X	X	X	X	X	X	X	
MA-02(02)	AUTOMATED MAINTENANCE ACTIVITIES	P2				X							X					
MA-03	**MAINTENANCE TOOLS**	P3			X	X					X	X	X	X	X		X	
MA-03(01)	INSPECT TOOLS	P3			X	X							X	X			X	
MA-03(02)	INSPECT MEDIA	P3			X	X							X	X		X	X	
MA-03(03)	PREVENT UNAUTHORIZED REMOVAL	P3				X							X	X		X		
MA-04	**NONLOCAL MAINTENANCE**	P2	X	X	X	X					X	X	X	X	X	X	X	X
MA-04(01)	AUDITING AND REVIEW	P2				X							X	X				
MA-04(02)	DOCUMENT NONLOCAL MAINTENANCE	P2			X	X							X	X	X		X	
MA-04(03)	COMPARABLE SECURITY / SANITIZATION	P2				X							X	X				

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
MA-04(06)	CRYPTOGRAPHIC PROTECTION	P2											X			X		
MA-04(07)	REMOTE DISCONNECT VERIFICATION	P0														X		
MA-05	**MAINTENANCE PERSONNEL**	P2	X	X	X	X					X	X	X	X	X	X	X	
MA-05(01)	INDIVIDUALS WITHOUT APPROPRIATE ACCESS	P2				X							X					
MA-05(04)	FOREIGN NATIONALS	P0														X		
MA-06	**TIMELY MAINTENANCE**	P2			X	X					X		X	X			X	
MP-01	**MEDIA PROTECTION POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	
MP-02	**MEDIA ACCESS**	P1	X	X	X	X					X	X	X	X	X	X	X	
MP-03	**MEDIA MARKING**	P2		X	X	X					X	X	X	X	X	X	X	X
MP-04	**MEDIA STORAGE**	P1		X	X	X	X				X	X	X	X	X	X	X	X
MP-05	**MEDIA TRANSPORT**	P1		X	X	X	X				X	X	X	X	X	X	X	X
MP-05(03)	CUSTODIANS	P1				X							X					
MP-05(04)	CRYPTOGRAPHIC PROTECTION	P1			X	X							X	X	X	X	X	
MP-06	**MEDIA SANITIZATION**	P1	X	X	X	X	X			TGC 2054.130	X	X	X	X	X	X	X	
MP-06(01)	REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY	P1				X							X	X	X	X		
MP-06(02)	EQUIPMENT TESTING	P1				X							X	X		X		
MP-06(03)	NONDESTRUCTIVE TECHNIQUES	P1				X							X			X		
MP-06(08)	REMOTE PURGING / WIPING OF INFORMATION	P1																
MP-07	**MEDIA USE**	P1	X	X	X	X					X		X	X		X	X	
MP-07(01)	PROHIBIT USE WITHOUT OWNER	P1			X	X							X	X		X	X	
MP-08(03)	CONTROLLED UNCLASSIFIED INFORMATION	P1											X					
MP-CMS-01	MEDIA RELATED RECORDS	P2											X	X				
PE-01	**PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
PE-02	**PHYSICAL ACCESS AUTHORIZATIONS**	P1	X	X	X	X	X				X	X	X	X	X	X	X	
PE-02(01)	ACCESS BY POSITION / ROLE	P1											X	X	X	X		
PE-02(03)	RESTRICT UNESCORTED ACCESS	P0														X		
PE-03	**PHYSICAL ACCESS CONTROL**	P1	X	X	X	X	X				X	X	X	X	X	X	X	
PE-03(01)	INFORMATION SYSTEM ACCESS	P1				X							X					
PE-03(02)	FACILITY / INFORMATION SYSTEM BOUNDARIES	P0														X		
PE-03(03)	CONTINUOUS GUARDS / ALARMS / MONITORING	P0														X		
PE-04	**ACCESS CONTROL FOR TRANSMISSION MEDIUM**	P1			X	X					X	X	X	X	X	X	X	
PE-05	**ACCESS CONTROL FOR OUTPUT DEVICES**	P2			X	X	X				X	X	X	X	X	X	X	
PE-06	**MONITORING PHYSICAL ACCESS**	P1	X	X	X	X					X	X	X	X	X	X	X	
PE-06(01)	INTRUSION ALARMS / SURVEILLANCE EQUIPMENT	P1			X	X							X	X	X	X	X	
PE-06(04)	MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS	P1				X							X					
PE-08	**VISITOR ACCESS RECORDS**	P3	X	X	X	X					X	X	X	X	X	X	X	
PE-08(01)	AUTOMATED RECORDS MAINTENANCE / REVIEW	P3				X							X					
PE-09	**POWER EQUIPMENT AND CABLING**	P1			X	X					X	X	X	X			X	
PE-10	**EMERGENCY SHUTOFF**	P1			X	X					X	X	X	X			X	
PE-11	**EMERGENCY POWER**	P1			X	X					X	X	X	X			X	
PE-11(01)	LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY	P1				X							X					
PE-12	**EMERGENCY LIGHTING**	P1	X	X	X	X					X	X	X	X			X	
PE-13	**FIRE PROTECTION**	P1	X	X	X	X					X	X	X	X			X	
PE-13(01)	DETECTION DEVICES / SYSTEMS	P1				X							X	X				
PE-13(02)	SUPPRESSION DEVICES / SYSTEMS	P1				X							X	X				
PE-13(03)	AUTOMATIC FIRE SUPPRESSION	P1			X	X							X	X			X	
PE-14	**TEMPERATURE AND HUMIDITY CONTROLS**	P1	X	X	X	X					X	X	X	X			X	
PE-14(02)	MONITORING WITH ALARMS / NOTIFICATIONS	P1											X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
PE-15	**WATER DAMAGE PROTECTION**	P1	X	X	X	X					X	X	X	X			X	
PE-15(01)	AUTOMATION SUPPORT	P1				X							X					
PE-16	**DELIVERY AND REMOVAL**	P2	X	X	X	X					X	X	X	X	X		X	
PE-17	**ALTERNATE WORK SITE**	P2			X	X					X	X	X	X	X	X	X	
PE-18	**LOCATION OF INFORMATION SYSTEM COMPONENTS**	P3			X	X					X	X	X	X	X	X		
PE-18(01)	FACILITY SITE	P3				X							X			X		
PE-19	**INFORMATION LEAKAGE**											X						
PE-20	**ASSET MONITORING AND TRACKING**	P0										X				X		
PL-01	**SECURITY PLANNING POLICY AND PROCEDURES**	P1	X	X	X	X				TAC 202.20(3);	X	X	X	X	X	X	X	
PL-02	**SYSTEM SECURITY PLAN**	P1	X	X	X	X					X	X	X	X	X	X	X	
PL-02(03)	PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	P1			X	X							X	X		X	X	
PL-04	**RULES OF BEHAVIOR**	P2	X	X	X	X	X			TAC 202.22(3); TGC 2054.134	X		X	X	X	X	X	
PL-04(01)	SOCIAL MEDIA AND NETWORKING RESTRICTIONS	P2			X	X	X						X	X	X	X	X	
PL-07	**SECURITY CONCEPT OF OPERATIONS**	P0														X		
PL-08	**INFORMATION SECURITY ARCHITECTURE**	P1			X	X					X	X	X	X		X	X	
PL-09	**CENTRAL MANAGEMENT**	P0														X		
PM-01	**INFORMATION SECURITY PROGRAM PLAN**	P1	X	X	X	X				TAC 202.20(5); TAC 202.20(7); TAC 202.21(b)(1); TAC 202.21(b)(11); TAC 202.21(b)(12); TAC 202.23(b)(3); TAC 202.26(c); TGC 2054.133	X	X	X	X		X	X	
PM-02	**SENIOR INFORMATION SECURITY OFFICER**	P1	X	X	X	X	X			TAC 202.20(1); TAC 202.21(a); TAC 202.21(b)(2-3, 5)	X		X	X	X		X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
PM-03	**INFORMATION SECURITY RESOURCES**	P1	X	X	X	X				TAC 202.20(2); TAC 202.23(a)(3)	X		X	X			X	
PM-04	**PLAN OF ACTION AND MILESTONES PROCESS**	P1	X	X	X	X				TAC 202.24(a)(5)	X	X	X	X			X	
PM-05	**INFORMATION SYSTEM INVENTORY**	P1	X	X	X	X				TAC 202.21(b)(7); TGC 2054.0965	X		X	X			X	X
PM-06	**INFORMATION SECURITY MEASURES OF PERFORMANCE**	P1	X	X	X	X				TAC 202.23(a)(1)	X	X	X	X			X	X
PM-07	**ENTERPRISE ARCHITECTURE**	P1	X	X	X	X					X		X	X			X	
PM-08	**CRITICAL INFRASTRUCTURE PLAN**	P1	X	X	X	X					X	X	X	X			X	
PM-09	**RISK MANAGEMENT STRATEGY**	P1	X	X	X	X				TAC 202.23(a)(2); TAC 202.25; TGC 2057.077	X	X	X	X			X	
PM-10	**SECURITY AUTHORIZATION PROCESS**	P1			X	X					X		X	X			X	
PM-11	**MISSION/BUSINESS PROCESS DEFINITION**	P1	X	X	X	X					X	X	X	X			X	
PM-12	**INSIDER THREAT PROGRAM**	P1	X	X	X	X					X	X	X	X			X	
PM-13	**INFORMATION SECURITY WORKFORCE**	P1	X	X	X	X				TAC 202.20(4)	X	X	X	X			X	X
PM-14	**TESTING, TRAINING, AND MONITORING**	P1	X	X	X	X					X	X	X	X			X	X
PM-15	**CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**	P3	X	X	X	X					X	X	X	X			X	X
PM-16	**THREAT AWARENESS PROGRAM**	P1	X	X	X	X					X	X	X	X			X	
PS-01	**PERSONNEL SECURITY POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	
PS-02	**POSITION RISK DESIGNATION**	P2	X	X	X	X					X	X	X	X	X	X	X	
PS-03	**PERSONNEL SCREENING**	P1	X	X	X	X					X	X	X	X	X	X	X	
PS-03(01)	CLASSIFIED INFORMATION	P0														X		
PS-03(02)	FORMAL INDOCTRINATION	P0														X		
PS-03(03)	INFORMATION WITH SPECIAL PROTECTION MEASURES	P1											X			X		
PS-04	**PERSONNEL TERMINATION**	P2	X	X	X	X					X	X	X	X	X	X	X	
PS-04(02)	AUTOMATED NOTIFICATION	P1				X							X					
PS-05	**PERSONNEL TRANSFER**	P2	X	X	X	X					X	X	X	X	X	X	X	
PS-06	**ACCESS AGREEMENTS**	P3	X	X	X	X				TGC 2054.134	X	X	X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
PS-06(02)	CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION	P0														X		
PS-07	**THIRD-PARTY PERSONNEL SECURITY**	P1	X	X	X	X	X				X	X	X	X	X	X	X	
PS-08	**PERSONNEL SANCTIONS**	P3	X	X	X	X					X	X	X	X	X	X	X	
RA-01	**RISK ASSESSMENT POLICY AND PROCEDURES**	P1	X	X	X	X				TAC 202.22	X	X	X	X	X		X	
RA-02	**SECURITY CATEGORIZATION**	P1	X	X	X	X				TAC 202.22(1)(A)	X	X	X	X			X	X
RA-03	**RISK ASSESSMENT**	P1	X	X	X	X				TAC 202.21(b)(6); TAC 202.24(a)(1); TAC 202.25(1-3)	X	X	X	X	X	X	X	
RA-05	**VULNERABILITY SCANNING**	P1	X	X	X	X					X	X	X	X	X	X	X	X
RA-05(01)	UPDATE TOOL CAPABILITY	P1			X	X							X	X	X	X	X	
RA-05(02)	UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED	P1			X	X							X	X		X	X	
RA-05(03)	BREADTH / DEPTH OF COVERAGE	P1				X							X	X		X		
RA-05(04)	DISCOVERABLE INFORMATION	P1				X							X					
RA-05(05)	PRIVILEGED ACCESS	P1			X	X							X	X		X	X	
RA-05(06)	AUTOMATED TREND ANALYSES	P1											X					
RA-05(08)	REVIEW HISTORIC AUDIT LOGS	P1											X					
SA-01	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**	P1	X	X	X	X					X		X	X	X		X	
SA-02	**ALLOCATION OF RESOURCES**	P1	X	X	X	X				TAC 202.20(2)	X		X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
SA-03	**SYSTEM DEVELOPMENT LIFE CYCLE**	P1	X	X	X	X	X			TAC 202.20(8); TAC 202.21(b)(3); TAC 202.21(b)(8); TAC 202.22(1); TAC 202.22(2); TAC 204.24; TGC 2054.112	X	X	X	X	X		X	
SA-04	**ACQUISITION PROCESS**	P1	X	X	X	X				TAC 202.21(b)(9); TAC 202.21(b)(10)	X	X	X	X	X	X	X	X
SA-04(01)	FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	P1			X	X							X	X	X	X	X	
SA-04(02)	DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS	P1			X	X							X	X			X	
SA-04(08)	CONTINUOUS MONITORING PLAN	P1											X					
SA-04(09)	FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE	P1			X	X							X	X		X	X	
SA-04(10)	USE OF APPROVED PIV PRODUCTS	P1				X							X				X	
SA-05	**INFORMATION SYSTEM DOCUMENTATION**	P2	X	X	X	X					X	X	X	X	X	X	X	
SA-08	**SECURITY ENGINEERING PRINCIPLES**	P1			X	X					X	X	X	X	X		X	
SA-09	**EXTERNAL INFORMATION SYSTEM SERVICES**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
SA-09(01)	RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS	P1											X	X		X		
SA-09(02)	IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES	P1			X	X							X	X		X	X	
SA-09(04)	CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	P1											X					
SA-09(05)	PROCESSING, STORAGE, AND SERVICE LOCATION	P1		X	X	X	X						X	X				
SA-10	**DEVELOPER CONFIGURATION MANAGEMENT**	P1		X	X	X	X				X	X	X	X	X	X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
SA-10(01)	SOFTWARE / FIRMWARE INTEGRITY VERIFICATION	P1											X					
SA-11	**DEVELOPER SECURITY TESTING AND EVALUATION**	P2		X	X	X		X		TGC 2054.516	X	X	X	X	X	X	X	X
SA-11(01)	STATIC CODE ANALYSIS	P1			X	X		X		TGC 2054.516			X	X		X		
SA-11(02)	THREAT AND VULNERABILITY ANALYSES	P1			X	X		X		TGC 2054.516			X					
SA-11(05)	PENETRATION TESTING	P2			X	X		X		TGC 2054.516			X					
SA-11(08)	DYNAMIC CODE ANALYSIS	P1			X	X		X		TGC 2054.516			X					
SA-12	**SUPPLY CHAIN PROTECTION**	P1				X					X	X	X					
SA-12(02)	SUPPLIER REVIEWS	P0														X		
SA-13	**TRUSTWORTHINESS**	P2				X							X					X
SA-14	**CRITICALITY ANALYSIS**											X						
SA-15	**DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**	P2				X					X	X	X					X
SA-15(09)	USE OF LIVE DATA	P2											X					
SA-16	**DEVELOPER-PROVIDED TRAINING**	P2				X					X		X					X
SA-17	**DEVELOPER SECURITY ARCHITECTURE AND DESIGN**	P1			X	X					X	X	X					X
SA-21	**DEVELOPER SCREENING**	P1				X							X					X
SA-22	**UNSUPPORTED SYSTEM COMPONENTS**	P1				X							X	X	X			
SC-01	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**	P1	X	X	X	X					X		X	X	X		X	
SC-02	**APPLICATION PARTITIONING**	P1			X	X					X		X	X	X	X	X	
SC-02(01)	INTERFACES FOR NON-PRIVILEGED USERS	P0														X		
SC-03	**SECURITY FUNCTION ISOLATION**	P1				X					X		X			X		
SC-03(02)	ACCESS / FLOW CONTROL FUNCTIONS	P1				X							X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
SC-03(03)	MINIMIZE NONSECURITY FUNCTIONALITY	P1				X							X					
SC-03(04)	MODULE COUPLING AND COHESIVENESS	P1				X							X					
SC-03(05)	LAYERED STRUCTURES	P1				X							X					
SC-04	**INFORMATION IN SHARED RESOURCES**	P1			X	X					X		X	X	X	X	X	
SC-05	**DENIAL OF SERVICE PROTECTION**	P1	X	X	X	X					X	X	X	X	X	X	X	
SC-05(01)	RESTRICT INTERNAL USERS	P0														X		
SC-05(02)	EXCESS CAPACITY / BANDWIDTH / REDUNDANCY	P0														X		
SC-05(03)	DETECTION / MONITORING	P0														X		
SC-06	**RESOURCE AVAILABILITY**	P0											X	X		X		
SC-07	**BOUNDARY PROTECTION**	P1	X	X	X	X					X	X	X	X	X	X	X	X
SC-07(03)	ACCESS POINTS	P1			X	X							X	X	X	X	X	
SC-07(04)	EXTERNAL TELECOMMUNICATIONS SERVICES	P1			X	X							X	X	X	X	X	
SC-07(05)	DENY BY DEFAULT / ALLOW BY EXCEPTION	P1			X	X							X	X	X	X	X	
SC-07(07)	PREVENT SPLIT TUNNELING FOR REMOTE DEVICES	P1			X	X							X	X	X	X	X	
SC-07(08)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	P1				X							X	X		X		
SC-07(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC	P0														X		
SC-07(12)	HOST-BASED PROTECTION	P1											X	X		X		
SC-07(13)	ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS	P1											X	X		X		
SC-07(14)	PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS	P1											X			X		
SC-07(18)	FAIL SECURE	P1				X							X	X		X		
SC-07(19)	BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	P0														X		
SC-07(21)	ISOLATION OF INFORMATION SYSTEM COMPONENTS	P1				X							X					
SC-08	**TRANSMISSION CONFIDENTIALITY AND INTEGRITY**	P1			X	X	X	X			X	X	X	X	X	X	X	X

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
SC-08(01)	CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION	P1			X	X							X	X	X	X	X	
SC-08(02)	PRE / POST TRANSMISSION HANDLING	P1				X							X	X		X		
SC-10	**NETWORK DISCONNECT**	P2			X	X					X		X	X	X	X	X	
SC-11	**TRUSTED PATH**	P0														X		
SC-12	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**	P1	X	X	X	X		X			X	X	X	X	X	X	X	
SC-12(01)	AVAILABILITY	P1				X							X			X		
SC-12(02)	SYMMETRIC KEYS	P1											X	X		X		
SC-12(03)	ASYMMETRIC KEYS	P1											X			X		
SC-13	**CRYPTOGRAPHIC PROTECTION**	P1	X	X	X	X	X				X	X	X	X	X	X	X	
SC-15	**COLLABORATIVE COMPUTING DEVICES**	P1	X	X	X	X					X		X	X	X	X	X	X
SC-15(01)	PHYSICAL DISCONNECT	P1				X							X			X		
SC-16	**TRANSMISSION OF SECURITY ATTRIBUTES**	P0														X		X
SC-16(01)	INTEGRITY VALIDATION	P0														X		
SC-17	**PUBLIC KEY INFRASTRUCTURE CERTIFICATES**	P1		X	X	X					X		X	X	X	X	X	X
SC-18	**MOBILE CODE**	P2		X	X	X					X	X	X	X	X	X	X	X
SC-18(01)	IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS	P0														X		
SC-18(02)	ACQUISITION / DEVELOPMENT / USE	P0														X		
SC-18(03)	PREVENT DOWNLOADING / EXECUTION	P0														X		
SC-18(04)	PREVENT AUTOMATIC EXECUTION	P0														X		
SC-19	**VOICE OVER INTERNET PROTOCOL**	P1			X	X					X		X	X	X	X	X	
SC-20	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**	P1	X	X	X	X					X		X	X		X	X	X
SC-21	**SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)**	P1	X	X	X	X					X		X	X		X	X	X
SC-22	**ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE**	P1	X	X	X	X					X		X	X		X	X	
SC-23	**SESSION AUTHENTICITY**	P1		X	X	X					X		X	X	X	X	X	X

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
SC-23(01)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT	P0														X		
SC-23(03)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION	P0														X		
SC-24	**FAIL IN KNOWN STATE**	P1				X					X		X			X		X
SC-28	**PROTECTION OF INFORMATION AT REST**	P1		X	X	X	X	X			X	X	X	X	X	X	X	X
SC-28(01)	CRYPTOGRAPHIC PROTECTION	P1		X	X	X		X					X			X		
SC-31	**COVERT CHANNEL ANALYSIS**											X						X
SC-32	**INFORMATION SYSTEM PARTITIONING**	P1				X							X	X		X		
SC-36	**DISTRIBUTED PROCESSING AND STORAGE**	P0														X		
SC-37	**OUT-OF-BAND CHANNELS**	P0														X		
SC-37(01)	ENSURE DELIVERY / TRANSMISSION	P0														X		
SC-38	**OPERATIONS SECURITY**	P0														X		
SC-39	**PROCESS ISOLATION**	P1	X	X	X	X					X		X	X			X	X
SC-40	**WIRELESS LINK PROTECTION**	P0														X		X
SC-43	**USAGE RESTRICTIONS**	P0														X		
SC-44	**DETONATION CHAMBERS**											X						X
SC-CMS-01	**ELECTRONIC MAIL**	P2											X					
SC-CMS-02	**WEBSITE USAGE**	P2											X					
SC-ACA-01	**ELECTRONIC MAIL**	P0												X				
SC-ACA-02	**FAX USAGE**	P0												X				
SI-01	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**	P1	X	X	X	X					X	X	X	X	X	X	X	
SI-02	**FLAW REMEDIATION**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
SI-02(01)	CENTRAL MANAGEMENT	P1				X							X	X	X			
SI-02(02)	AUTOMATED FLAW REMEDIATION STATUS	P1			X	X							X	X		X	X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
SI-02(03)	TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS	P1											X			X		
SI-03	**MALICIOUS CODE PROTECTION**	P1	X	X	X	X	X				X	X	X	X	X	X	X	X
SI-03(01)	CENTRAL MANAGEMENT	P1			X	X							X	X	X	X	X	
SI-03(02)	AUTOMATIC UPDATES	P1			X	X							X	X	X	X	X	
SI-03(07)	NONSIGNATURE-BASED DETECTION	P1											X					
SI-04	**INFORMATION SYSTEM MONITORING**	P1	X	X	X	X					X	X	X	X	X	X	X	X
SI-04(01)	SYSTEM-WIDE INTRUSION DETECTION SYSTEM	P1				X							X	X		X		X
SI-04(02)	AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	P1			X	X							X	X		X	X	
SI-04(03)	AUTOMATED TOOL INTEGRATION	P1				X							X					X
SI-04(04)	INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	P1			X	X							X	X	X	X	X	
SI-04(05)	SYSTEM-GENERATED ALERTS	P1			X	X							X	X	X	X	X	
SI-04(07)	AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	P1													X	X		
SI-04(09)	TESTING OF MONITORING TOOLS	P1														X		
SI-04(11)	ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	P1														X		X
SI-04(12)	AUTOMATED ALERTS	P1													X	X		
SI-04(14)	WIRELESS INTRUSION DETECTION	P1				X							X	X	X	X		
SI-04(15)	WIRELESS TO WIRELINE COMMUNICATIONS	P1														X		
SI-04(16)	CORRELATE MONITORING INFORMATION	P1				X							X					
SI-04(23)	HOST-BASED DEVICES	P1				X							X		X			
SI-04(24)	INDICATORS OF COMPROMISE	P1				X							X					
SI-05	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**	P1	X	X	X	X					X	X	X	X	X	X	X	
SI-05(01)	AUTOMATED ALERTS AND ADVISORIES	P1				X							X			X		
SI-06	**SECURITY FUNCTION VERIFICATION**	P1				X							X	X				
SI-06(02)	AUTOMATION SUPPORT FOR DISTRIBUTED TESTING	P1				X							X					

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	**Control Name**	**Priority**	**Low**	**Low Plus**	**Mod**	**High**	**SPI**	**Web & Mobile**	**Cloud**	**Texas Code**	**DIR**	**HIPAA**	**CMS-ARS**	**CMS-MARS-E**	**IRS**	**CJIS**	**VA Mod**	**CIS Critical**
SI-07	**SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**	P1			X	X						X	X	X		X	X	
SI-07(01)	INTEGRITY CHECKS	P1			X	X							X	X		X	X	
SI-07(02)	AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS	P1				X							X					
SI-07(05)	AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	P1				X							X					
SI-07(06)	CRYPTOGRAPHIC PROTECTION	P1											X					
SI-07(07)	INTEGRATION OF DETECTION AND RESPONSE	P1			X	X							X	X		X	X	
SI-07(14)	BINARY OR MACHINE EXECUTABLE CODE	P1				X							X					
SI-08	**SPAM PROTECTION**	P2		X	X	X					X	X	X	X	X	X	X	
SI-08(01)	CENTRAL MANAGEMENT	P2			X	X							X	X		X	X	
SI-08(02)	AUTOMATIC UPDATES	P2			X	X							X	X		X	X	X
SI-10	**INFORMATION INPUT VALIDATION**	P1		X	X	X		X			X		X	X	X	X	X	
SI-11	**ERROR HANDLING**	P2		X	X	X		X			X		X	X	X	X	X	
SI-12	**INFORMATION HANDLING AND RETENTION**	P2	X	X	X	X					X		X	X	X	X	X	
SI-16	**MEMORY PROTECTION**	P1		X	X	X					X		X	X	X		X	
AP-01	**AUTHORITY TO COLLECT**	P1											X	X			X	
AP-02	**PURPOSE SPECIFICATION**	P1											X	X			X	
AP-CMS-01	**AUTHORITY AND PURPOSE CONTROL FAMILY POLICY AND PROCEDURE**	P1											X					
AR-01	**GOVERNANCE AND PRIVACY PROGRAM**	P1										X	X	X			X	
AR-02	**PRIVACY IMPACT AND RISK ASSESSMENT**	P1											X	X			X	
AR-03	**PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS**	P1											X	X			X	
AR-04	**PRIVACY MONITORING AND AUDITING**	P1											X	X			X	
AR-05	**PRIVACY AWARENESS AND TRAINING**	P1											X	X			X	
AR-06	**PRIVACY REPORTING**	P1											X	X			X	
AR-07	**PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT**	P1											X	X			X	
AR-08	**ACCOUNTING OF DISCLOSURES**	P1											X	X			X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
AR-CMS-01	ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT CONTROL FAMILY POLICY AND PROCEDURE	P1											X					
DI-01	DATA QUALITY	P1											X	X			X	
DI-01(01)	VALIDATE PII	P1											X	X				
DI-CMS-01	DATA QUALITY AND INTEGRITY CONTROL FAMILY POLICY AND PROCEDURES	P1											X					
DI-02	DATA INTEGRITY AND DATA INTEGRITY BOARD	P1												X			X	
DM-01	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION	P1											X	X			X	
DM-01(01)	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION	P1												X				
DM-02	DATA RETENTION AND DISPOSAL	P1											X	X			X	
DM-02(01)	SYSTEM CONFIGURATION	P1											X	X				
DM-03	MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH	P1											X	X			X	
DM-03(01)	RISK MINIMIZATION TECHNIQUES	P1											X	X				
DM-CMS-01	DATA MINIMIZATION AND RETENTION CONTROL FAMILY POLICY AND PROCEDURES	P1											X					
IP-01	CONSENT	P1										X	X	X			X	
IP-01(01)	MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT	P1											X	X				
IP-02	INDIVIDUAL ACCESS	P1											X	X			X	
IP-03	REDRESS	P1											X	X			X	
IP-04	COMPLAINT MANAGEMENT	P1											X	X			X	
IP-04(01)	RESPONSE TIMES	P1											X	X				
IP-CMS-01	INDIVIDUAL PARTICIPATION AND REDRESS CONTROL FAMILY POLICY AND PROCEDURES	P1											X					
SE-01	INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	P1										X	X	X			X	

			Baselines				HHS Overlays			State Overlays		Federal Overlays						
Control ID	Control Name	Priority	Low	Low Plus	Mod	High	SPI	Web & Mobile	Cloud	Texas Code	DIR	HIPAA	CMS-ARS	CMS-MARS-E	IRS	CJIS	VA Mod	CIS Critical
SE-02	PRIVACY INCIDENT RESPONSE	P1											X	X			X	
SE-CMS-01	SECURITY CONTROL FAMILY POLICY AND PROCEDURES	P1											X					
TR-01	PRIVACY NOTICE	P1										X	X	X			X	
TR-01(01)	REAL-TIME OR LAYERED NOTICE	P1											X	X				
TR-02	SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS	P1											X	X			X	
TR-02(01)	PUBLIC WEBSITE PUBLICATION	P1											X	X				
TR-03	DISSEMINATION OF PRIVACY PROGRAM INFORMATION	P1											X	X			X	
TR-CMS-01	TRANSPARENCY CONTROL FAMILY POLICY AND PROCEDURES	P1											X					
UL-01	INTERNAL USE	P1										X	X	X			X	
UL-02	INFORMATION SHARING WITH THIRD PARTIES	P1											X	X			X	
UL-CMS-01	USE LIMITATION CONTROL FAMILY POLICY AND PROCEDURES	P1											X					

Appendix B: HHS Information Security Controls

For an explanation of how to use Appendix B refer to section 4.1.

(AC) ACCESS CONTROLS

The HHS organization requires limited access to applications, servers, databases, and network devices in the HHS environment. Access is limited to authorized users, processes acting on behalf of authorized users, or devices. Authorized users are further limited to the types of transactions and functions that they are permitted to exercise.

AC-01: ACCESS CONTROL POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates (as necessary) the current: 1. Access control policy at least once every three (3) years (or if there is significant change); and 2. Access control procedures at least every three hundred sixty-five (365) days. **CMS-MARS-E:** b.1. Access control policy at least once every three hundred sixty five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
HIPAA: Std.1 - The organization develops, disseminates, and reviews/updates the access control policies and procedures complying with the HIPAA Minimum Necessary Rule and permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PII: Access Control policies and procedures form the foundation that allows privacy protections to be implemented for the identified uses of personally identifiable information (PII) and protected health information (PHI). Privacy requirements commonly use the terms “adequate security” and “confidentiality” when referring to access controls and other security safeguards for PII. Applied together, these terms signify the need to make risk-based decisions based on the magnitude of harm (to both organizations and individuals) when determining applicable restrictions for PII. For the purpose of this overlay, refer to the definitions of “adequate security” in OMB Circular A-130, Appendix III, and “confidentiality” in NIST SP 800-37, Rev. 1, Appendix B. These definitions are consistent with Committee for National Security Systems Instruction (CNSSI) No. 4009.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Code: 5 United States Code (U.S.C.) §552a(b), (e)(9)-(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(3)(i), §164.308(a)(3)(ii)(A), §164.308(a)(4)(i), §164.308(a)(4)(ii)(B), §164.308(a)(4)(ii)(C), §164.312(a)(1), §164.514(d)(1)-(5); NIST SP: 800-12, 800-37 Rev. 1 Appendix B, 800-	PM-9, AR-4, AR-7, PE-1

100, 800-122; OMB Memo: M-06-16, M-07-16, Att. 4; OMB Circular A-130: 7.g. and Appendix III; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy and procedures; system security plan, other relevant documents or records.
Examine: Verify that the access control procedures are consistent with access control policy.
Examine: Verify that the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated access control controls.
Examine: Examine document transmission logs or audit logs or records to confirm that the access control policy and procedures have been disseminated or otherwise made available.
Examine: Examine policy and procedure documents to verify that responsible personnel are required to review the access control policy and procedures within the required timeframe and to update as necessary. Examine document changes, document revision records, after-action reports, etc., to ensure reviews were conducted.
Interview: Organizational personnel with access control responsibilities. Verify that personnel:
1. Confirm their respective roles with Access Control policy;
2. Know of and understand Access Control policy and procedures; and
3. Are responsible for reviewing and updating Access Control policy and procedures no less often than required.

AC-02: ACCOUNT MANAGEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, application, guest/anonymous, emergency, and temporary;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by defined personnel or roles (defined in the applicable security plan, normally Information Owners or Information Custodians) for requests to create information system accounts;
f. Creates, enables, modifies, disables, and removes information system accounts in accordance with HHS Standards and Procedures;
g. Monitors the use of information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements at least in accordance with implementation Std.8; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

CMS-ARS
j. Reviews accounts for compliance with account management requirements at least every 90 days for High and Moderate systems or 365 days for Low systems;

IRS
j. Reviews accounts for compliance with account management requirements at least every 180 days for privileged accounts and 365 days for non-privileged accounts.

CMS-MARS-E
j. Reviews accounts for compliance with account management requirements at least every 180 days for user accounts and 365 days for other accounts.

CONTROL IMPLEMENTATION STANDARDS

Low, Low Plus, Moderate, High
Std.1 - The Information Owner or his or her designated representative(s) are responsible for approving access to information resources and periodically reviewing access lists based on documented risk management decisions.
Std.2 - Remove or disable default user accounts. Rename active default accounts.
Std.3 - Implement centralized control of user access administrator functions.
Std.4 - Regulate the access provided to contractors and define security requirements for contractors.
Std.5 - Automated account management results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Account management information sources include systems, appliances, devices, services, and applications (including databases); and
(c) HHS Information Security-directed account management information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - Raw security information/results from automated account management tools must be available in an unaltered format to HHS Information Security.
Std.7 - Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.

Low
Std.8 – every 3 years

Low Plus
Std.8 – every 2 years

Moderate, High
Std.8 – every 365 days

SPI:
Std.9 - The Applicant/Bidder monitors and manages access to HHS Confidential Information (e.g., a formal process exists for granting access and validating the need for users to access HHS Confidential information, and access is limited to Authorized Users.

CMS-ARS:
Moderate, High:
Std.10 - Prohibit use of guest, anonymous, and shared accounts for providing access to PII.
Std.11 - Notify account managers within an organization-defined timeframe when temporary accounts are no longer required or when information system users are terminated or transferred or information system usage or need-to-know/need-to-share changes.
Std.12 - Prior to granting access to PII, users demonstrate a need for the PII in the performance of the user's duties.
Std.13 - Implement access controls within the information system based on users' or user group's need for access to PII in the performance of their duties.
Std.14 - Organizations should provide access only to the minimum amount of PII necessary for users to perform their duties.
Std.15 - Create, enable, modify, disable, and remove information system accounts in accordance with the requirement for each user to complete privacy training every 365 days, otherwise the account would be disabled.

Moderate:
Std.16 - Review accounts for compliance with account management requirements at least every 365 days.

High:
Std.16 - Review accounts for compliance with account management requirements at least quarterly for privileged accounts, at least every 365 days for general user's accounts.

SUPPLEMENTAL GUIDANCE

Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/Information Owner(s)/Custodian(s), or CISO) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training.

PII:
Account management is a critical function for developing and implementing an access control framework that is appropriate for the information contained in systems and applications. When implemented effectively, the access control framework provides the necessary constructs for controlling access to PII, limiting disclosure of records about individuals to only those system and application users that have a need for the information to perform their job functions. The purpose of this guidance is to establish requirements for user access to PHI and PII.

HIPAA:
The identification of authorized users and access privileges include considerations of whether the user will need access to PHI and whether such access may be permitted or required under HIPAA. The purpose of this guidance is to establish requirements for user access to PHI. Organizations should establish procedures for obtaining necessary electronic protected health information, to include during an emergency.

REFERENCES	RELATED CONTROLS
State: TAC 202.22 (1)(B); DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b), (e)(9)-(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.502; OMB Memo: M-07-16 Att. 1, M-16-04; IRS1075; CJIS 5.6	AC-3, AC-4, AC-5, AC-6, AC-10, AC-16, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, CM-11, IA-2, IA-4, IA-5, IA-8, MA-3, MA-4, MA-5, PL-4, SC-13

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing account management (including creating, enabling, modifying, reviewing, disabling, and removing accounts); system security plan; list of active information system accounts along with the name of the individual associated with each account; list of guest/anonymous and temporary accounts along with the name of the individual associated with the each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records.
Examine and Confirm:
1. The organization requires proper identification for all requests for information system access accounts; and
2. Account managers are notified when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes.

Examine: Information system demonstrates that policy is being implemented. Ensure: 1. Only authorized and necessary accounts are enabled; 2. Defined groups consist of only authorized users; 3. Non-interactive system accounts are locked down; 4. Access to privileged accounts is restricted to authorized users; and 5. Information system accounts are reviewed for compliance no less often than required. Interview: Organizational personnel with account management responsibilities. Ensure personnel know: 1. Access Control policy and procedures; 2. Responsibilities associated with account management; 3. Procedure/process for monitoring the use of guest/anonymous and temporary account; and 4. Organization must remove, disable, or otherwise secure unnecessary accounts. Test: Test an agreed-upon sample of mechanisms implementing account management functions to confirm that a comprehensive account management process is implemented to verify that only authorized users can gain access to workstations/laptops, applications and networks and the mechanisms are operating as intended and documented. View each "type" of account as documented in the system documentation by doing the following for each type of account: 1. Obtain an account on the system. This will demonstrate that a paper/review/decision process is in place to establish an account; 2. Access the account before it is activated. This should fail; 3. Access the account after its activation. This should pass; 4. Determine whether the password/authenticator was delivered in a secure manner; 5. Test (or have demonstrated) change in account privilege, change to group membership, change to authenticator (usually a password and it may not be on the system, for example, the password protecting a key store in a browser), and disabling (when possible); and 6. Test (or have demonstrated) the termination of an account. This includes assurance that proper record management is undertaken and completed.

AC-02(01): AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to support the management of information system accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated, transferred, or change their role; using the information system to monitor account usage; and using telephonic notification to report atypical information system account usage.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System security plan; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system demonstrates automated mechanisms are used to support the management of information system accounts. Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanisms.	

AC-02(02): REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS	
The information system automatically disables emergency accounts within 24 hours; and temporary accounts with a fixed duration not to exceed 30 days for High Systems and 365 days for Moderate Systems. **CMS-ARS:** The information system automatically disables emergency accounts within 24 hours; and temporary accounts with a fixed duration not to exceed 30 days for High Systems and 60 days for Moderate and Low Systems.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of active accounts; information system audit records; and other relevant documents or records. Examine: Information system demonstrates automated mechanisms are used to automatically disable temporary accounts and emergency accounts in defined time period. Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.	

AC-02(03): DISABLE INACTIVE ACCOUNTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system automatically disables inactive accounts within 30 days for High Systems or 90 days for Moderate Systems. **CMS-ARS, CMS-MARS-E:** The information system automatically disables inactive accounts within 30 days for High Systems or 60 days for Moderate and Low Systems.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; and other relevant documents or records. Examine: Information system demonstrates automated mechanisms are used to automatically disable inactive accounts in defined time period Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.	

AC-02(04): AUTOMATED AUDIT ACTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies defined personnel or roles (defined in the applicable security plan).	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Automated account management audit action results are made available to HHS Information Security: (a) Information must be searchable by HHS Information Security in a format compliant with HHS and federal (e.g., Continuous Diagnostics and Mitigation) requirements; and (b) Account management information sources include systems, appliances, devices, services, and applications (including databases). Std.2 - As required by HHS, raw security information/results from automated account management tools must be available in an unaltered format to HHS Information Security.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	AU-2, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System security plan; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system demonstrates enabled automated mechanisms that capture audit data on the defined account management actions. For example, verify that the system is configured to capture account creation, account modification, account enabling, account disabling, and account removal actions. Test: Automated mechanisms implementing account management functions. Review audit log to verify that the proper account management actions were taken and were recorded by automated mechanism.	

AC-02(05): INACTIVITY LOGOUT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, VA
CONTROL REQUIREMENTS	
The organization requires that users log out when the time-period of expected inactivity exceeds 90 minutes and at the end of the user's normal work period. **VA** The organization requires that users log off or lock any VA computer or console before walking away or initiate a comparable application feature that will keep others from accessing the information and resources available.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	SC-23
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; security violation reports; information system audit records; and other relevant documents or records.	

Examine: Information system demonstrates enabled automated mechanisms that regulate automated log-out for inactivity and enforcement of work-day access restrictions. Inspect organizational personnel workstations after hours to verify users have logged out. Interview: Organizational personnel with account management responsibilities. Test: Automated mechanisms implementing inactivity and work-day time restrictions.

AC-02(07): ROLE-BASED SCHEMES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
CMS-ARS: The organization: a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; b. Monitors privileged role assignments; and c. Inspects administrator groups, root accounts and other system related accounts on demand, but no less often than once every fourteen (14) calendar days to ensure that unauthorized accounts have not been created. **CMS-MARS-E:** a. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; b. The organization monitors privileged role assignments as well as application-specific privileged role assignments. c. The organization inspects administrator groups, root accounts, and other system-related accounts on demand, and at least once every fourteen (14) days to ensure that unauthorized accounts have not been created. Privileged user roles associated with applications should be inspected every thirty (30) days. d. The organization establishes and administers application-specific privileged user accounts in accordance with a role-based access scheme that allows access based on user responsibilities associated with application use.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; and other relevant documents or records. Examine: Information system demonstrates automated mechanisms implementing role-based access controls (e.g., role-based schema). Confirm that the organization has detailed procedures for establishing and administering accounts in accordance with role-based policy. Confirm information system monitors privileged role assignments. Interview: Organizational personnel with account management responsibilities. Test: Access to role-based functions is limited to authorized roles. Verify that defined functions and commands can be performed only by users with a specific role. Verify organizationally specified actions are taken when privileged role assignments are no longer appropriate.	

AC-02(09): RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS

Priority: P1

Baseline(s):	Overlay(s):CMS-ARS (Cloud Only)
CONTROL REQUIREMENTS	
The organization only permits the use of shared/group accounts when a business need can be documented and approved, in advance, by the Authorizing Official (AO). a. When shared/group accounts are used, the System Security Plan (SSP) must: 1. Describe how the shared/group accounts are used; and 2. Include compensating processes and procedures implemented to provide the ability to uniquely attribute account user activities.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – PII: The organization only permits the use of shared/group accounts that meet the requirement to uniquely attribute user activity to an account.	
SUPPLEMENTAL GUIDANCE	
Shared/group accounts do not provide the necessary accountability (such as non-repudiation) required to log and monitor access to sensitive information nor do they permit identification of individuals who have a need for access. Shared/group accounts also do not provide audit trails capable of associating a user with an action—eliminating the ability to establish non-repudiation. (Non-repudiation is a critical element of accountability and accuracy of information in systems, database or system history, and related logs and is important for investigating privacy incidents and breaches.) PII: Access to PII is more effectively controlled when access controls are considered during system design and built-into or enforced by the system (i.e., automated controls). Shared/group accounts that do not allow for uniquely attributing user activities should not be used for information systems that contain PII or PHI. Shared/group accounts do not allow for the necessary accountability (such as non-repudiation) required to log and monitor access to PII and PHI nor do they permit identification of individuals who have a need for access. Shared/group accounts do not permit audit trails to associate a user with an action, eliminating the ability to establish non-repudiation. Non-repudiation is a critical element of accountability and accuracy of information in systems, database or system history, and related logs and is important for investigating privacy incidents and breaches. Refer to RMH for account management process and procedures.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **Federal:** Code: 5 U.S.C. §552a(b)(1); 5 U.S.C. §552a(c)(1); FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(C), 45 C.F.R. §164.310(a)(2)(iii), 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(1), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv); OMB Circular A-130: 7.g. and 8.a.1, 8.b.(2)(c).	AC-14, AR-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts; information system audit records; and other relevant documents or records. Examine: Information system only implements shared/group accounts mechanisms approved by the AO and documented within the system security plan. Examine AO approval documents for shared accounts, if applicable. Interview: Organizational personnel with account management responsibilities. Ensure shared account users are using accounts as authorized by AO. Test: Automated mechanisms implementing account management functions.	

AC-02(10): SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS (Cloud Only)

CONTROL REQUIREMENTS	
The information system updates shared/group account credentials when members leave the group.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing access enforcement; system security plan; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; and other relevant documents or records. Examine: Information system requires password changes for shared accounts used by user who no longer needs access to the shared accounts. Test: Automated mechanisms implementing account management functions.	

AC-02(11): USAGE CONDITIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system enforces organizationally defined usage conditions and/or circumstances (as defined in the SSP) for organizationally defined information system accounts.	
CONTROL IMPLEMENTATION STANDARDS	
Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing access enforcement; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; and other relevant documents or records. Examine: Verify information system enforces organizationally defined usage conditions. Interview: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. Ensure personnel know system usage limitations. Test: Ensure automated mechanisms implement account management functions (i.e., usage restrictions are enabled and working).	

AC-02(12): ACCOUNT MONITORING / ATYPICAL USAGE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Monitors information system accounts for atypical use; and	

b. Reports atypical usage of information system accounts to defined personnel or roles (defined in the applicable security plan), and if necessary, incident response team.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	CA-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedures addressing account management; system security plan; documentation defining typical/normal use; information system configuration settings and associated documentation; information system audit records; audit tracking and monitoring reports; and other relevant documents or records. Examine: Information system implements functionality that assists in the detection of atypical use (change in behavior, unusual behavior, etc.) conditions. Examine audit logs or notification trail. Review notifications to specified personnel about user behavior. Interview: Organizational personnel with account management responsibilities, or information security responsibilities. Test: Automated mechanisms implementing account management functions. Examine audit logs or notification trail.	

AC-02(13): DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, VA
CONTROL REQUIREMENTS	
The organization disables accounts of users posing a significant risk immediately, not to exceed 30 minutes for High systems or 60 minutes for Moderate systems after discovery of the risk. **VA** The organization disables accounts of users posing a significant risk immediately after discovery of the risk.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between AOs, information system administrators, and HR managers is essential for timely execution of this control enhancement. Disabling accounts for high-risk individuals is a minimum requirement for the organization's rules of behavior as a consequence for abusing access privileges to access sensitive information, including information protected under the Privacy Act of 1974.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: Acceptable Use Policy (AUP), Acceptable Use Agreement (AUA) **Federal:** 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(1)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(C), Code: 5 U.S.C. §552a(e)(9)-(10); OMB Memo: M-07-16, M-16-04	PS-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Procedures addressing account management; system security plan; information system configuration settings and associated documentation; information system audit records; audit tracking and monitoring reports; and other relevant documents or records. Examine: Information system implements functionality that assists in disabling accounts if a user (or system account) is found to pose an unacceptable risk. Review notifications to specified personnel about user risk. Interview: Organizational personnel with account management responsibilities, or information security responsibilities. Test: Automated mechanisms implementing account management functions. Verify account is disabled within required timeframe following simulated user risk assessment.

AC-03: ACCESS ENFORCEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **IRS:** b. A role-based access control policy over defined subjects and objects and controls access to FTI based upon a valid access authorization, intended system usage, and the authority to be disclosed FTI under the provisions of IRC 6103.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - If encryption is used as an access control mechanism it must meet HHS approved (FIPS 140-2 compliant) encryption standards (see SC-13). **CMS-ARS, CMS-MARS-E, IRS, CJIS:** Std.1 - If encryption is used as an access control mechanism it must meet HHS approved (FIPS 140-2 validated) encryption standards (see SC-13). **CMS-ARS, CMS-MARS-E:** Std.2 - Configure operating system controls to disable public “read” and “write” access to all system files, objects, and directories. Configure operating system controls to disable public “read” access to files, objects, and directories that contain sensitive information. Std.3 - Data stored in the information system must be protected with system access controls and must be encrypted when residing in non-secure areas. **CMS-MARS-E:** Std.4 - When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.	
SUPPLEMENTAL GUIDANCE	
Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Well-designed, automated access controls (e.g., mandatory access control [MAC], discretionary access control [DAC], role-based access control [RBAC], or attribute-based access control [ABAC]) limit user access to information according to defined access policies, which helps ensure the security and confidentiality of sensitive information contained in the system. FIPS 140-2 validation certificate numbers are listed at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm PII:	

Well-designed, automated access controls (e.g., MAC, DAC, RBAC, or ABAC limit user access to information according to defined access policies, which helps ensure the security and confidentiality of the sensitive information, such as PII and PHI, contained in the system. For example, implement role-based access controls and configure access controls so that each user can access only the pieces of information necessary for the user's role or only permit users to access PII through an application that restricts their access to the PII the users require, instead of allowing users direct access to a database or files containing PII.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(a)(2)(ii), 45 C.F.R. §164.312(a)(2)(iv); OMB Memo: M-06-16 IRS1075-Sep2016 9.3.1.3; CJIS 5.6	AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing access enforcement; system security plan; information system configuration settings and associated documentation; list of approved authorizations (user privileges); information system audit records; if cryptography is implemented, FIPS 140-2 validation certificate number(s); other relevant documents or records. The access control procedures should specify the process for obtaining authorization as a requirement prior to gaining access to the information system. Examine: Information system implements functionality that enforces access controls. Examples: - RBACs - DACs - MACs - usage limitations - connection limitations - restrictions to functions with elevated privileges - restrictions to critical system functions (e.g., boot functions/basic input output system [BIOS]) Examine: Examine the information system access control configuration parameters (e.g., access control lists [ACL], file permissions, group definitions, and user profiles), including a review of file systems and data management systems to verify that they are configured in accordance with access control policy and procedures. Test: Automated mechanisms implementing access enforcement functions. Test a sample of system mechanisms that implement access control to confirm that the mechanisms are operating in accordance with policy and procedures. This control applies to applications with an integrated access control mechanism, such as WinZip and SecureZip, as well as the underlying operating system. These applications must meet requirements (FIPS 140-2 compliant module).	

AC-03(03): MANDATORY ACCESS CONTROL

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system enforces [Assignment: organization-defined mandatory access control policy] over all subjects and objects where the policy: a. Is uniformly enforced across all subjects and objects within the boundary of the information system; b. Specifies that a subject that has been granted access to information is constrained from doing any of the following; (1) Passing the information to unauthorized subjects or objects; (2) Granting its privileges to other subjects;	

(3) Changing one or more security attributes on subjects, objects, the information system, or information system components;
(4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or
(5) Changing the rules governing access control; and

c. Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges (i.e., they are trusted subjects)] such that they are not limited by some or all of the above constraints.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3(4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3(4), but policies governed by this control take precedence over the less rigorous constraints of AC-3(4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3(4) permits the subject to pass the information to any subject with the same sensitivity label as the subject.

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	AC-25, SC-11

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; mandatory access control policies; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of mandatory access control policies; information system audit records; other relevant documents or records.
Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.
Test: Automated mechanisms implementing mandatory access control.

AC-03(04): DISCRETIONARY ACCESS CONTROL

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system enforces [Assignment: organization-defined discretionary access control policy] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following:
(a) Pass the information to any other subjects or objects;
(b) Grant its privileges to other subjects;

(c) Change security attributes on subjects, objects, the information system, or the information system's components;
(d) Choose the security attributes to be associated with newly created or revised objects; or
(e) Change the rules governing access control.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. This control enhancement can operate in conjunction with AC-3(3). A subject that is constrained in its operation by policies governed by AC-3(3) is still able to operate under the less rigorous constraints of this control enhancement. Thus, while AC-3(3) imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, AC-3(4) permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside of the control of the information system, additional means may be required to ensure that the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

REFERENCES	RELATED CONTROLS
CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; discretionary access control policies; procedures addressing access enforcement; security plan; information system design documentation; information system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of discretionary access control policies; information system audit records; other relevant documents or records.
Interview: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.
Test: Automated mechanisms implementing discretionary access control policy.

AC-03(09): CONTROLLED RELEASE

Priority: P1

Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E

CONTROL REQUIREMENTS

The information system does not release information outside of the established system boundary unless both of the following are meet:
a. The receiving external organization (i.e., department, agency, or commercial entity not managed by HHS) provides information security and privacy safeguards commensurate with those implemented by HHS; and
b. HHS-defined information security and privacy safeguards (consistent with 45 CFR §155.260 Paragraph (b)(2)) are used to validate the appropriateness of the information designated for release.

PII:
The information system does not release information outside of the established system boundary unless:
a. The receiving organization or information system provides privacy and security controls commensurate with the PII confidentiality impact level of the PII being received; and
b. Controls UL-01 and UL-02 are used to validate the appropriateness of the information designated for release.

CONTROL IMPLEMENTATION STANDARDS

PII:
Std.1 - PII may only be released when authorized, there is a need to know, and adequate assurances of protection have been provided.
Std.2 - Applicable policy mandates establishing policy regarding access to PII, including PHI, are the Privacy Act of 1974,E-Government Act of 2002 (Section 208), and HIPAA.

SUPPLEMENTAL GUIDANCE

PII released outside a system boundary may be at increased risk for unauthorized access and use (i.e., a breach). Such release could include a formal process or an informal activity, such as a spreadsheet receiving data extracted from an information system. Applicable policy mandates establishing policy regarding access to PII, including PHI, are the Privacy Act of 1974,E-Government Act of 2002 (Section 208), and HIPAA.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(a)(7), (b), (c), (e)(3)(c), (o); Privacy: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment, Overview	AC-21, UL-01, UL-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing information sharing; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system implements functionality that restricts release of information outside of the established system boundary without pre-approval. Examine information system assessment and authorization documentation relative to security and privacy safeguards; and assess safeguards for adequacy. Test: Automated mechanisms implementing access enforcement functions. Verify unauthorized transfer attempts are detected and prevented.	

AC-04: INFORMATION FLOW ENFORCEMENT

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. **IRS:** Additional requirements for protecting the flow of FTI can be found in IRS 1075 Section 9.4.3, Email Communications, Section 9.4.4, Fax Equipment, and Section 9.4.9, Multi-Functional Devices	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to	

information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products.

CMS-ARS:
Security policy filters, or like technology, such as data loss prevention (DLP), can provide a form of continuous monitoring for compliance with privacy laws and regulations. Implementation of this security control reduces the potential for unauthorized transfer of PII.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b); NIST SP: 800-47; OMB Memo: M-06-19, M-07-16 Web: ucdmo.gov; IRS1075; CJIS 5.6	AC-3, AC-16, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

CMS-ARS:
Determine if:
(i) the organization defines security policy filters to be used as a basis for enforcing flow control decisions;
(ii) the organization defines information flows for which flow control decisions are to be applied and enforced; and
(iii) the information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions for organization-defined information flows.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records. Ensure that the system documentation describes:
1. The process for ensuring that each user receives only authorized information;
2. How the system processes all data traversing the network interface according to the applied access policy and/or filtering mechanism; and
3. Any requirements of boundary defense mechanisms at layered or internal enclave boundaries.
Examine: Information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. Examples:
- RBAC/MAC enabled;
- Networking is configured to enforce intended routing (e.g., disabling proxy/source/ redirect routing, IP spoofing, broadcasting);
- Ipv6 is disabled unless explicitly authorized; and
- Firewall rules adhere to a deny-all, permit-by-exception policy.
Examine: Confirm that the system design is capable of enforcing assigned authorizations for controlling the flow of information within the system and between interconnected systems. The system must verify that only data that is explicitly permitted (based on the filtering policies) is released from one network enclave to another network enclave.
Interview: Administration personnel knowledge of information flow and interconnection processes and procedures.
Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Test a specific sample of the information system automated mechanisms implementing information flow enforcement policy to confirm that the mechanisms are operating as intended. Attempt to send information to improper destinations (systems or users). Verify that the system detects the impermissible flow, prevents it, audits the violation, and notifies the appropriate personnel.

CMS-ARS:
Examine: Access control policy; information flow control policies; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and

associated documentation; list of security policy filters regulating flow control decisions; information system audit records; and other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers. Test: Automated mechanisms implementing information flow enforcement policy.

AC-04(08): SECURITY POLICY FILTERS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system enforces information flow control using best available security policy filters, or like technology to filter on selected PII values as a basis for flow control decisions for prevention of unauthorized transfer of PII across information system boundaries or domains.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Security policy filters, or like technology, such as data loss prevention (DLP), can provide a form of continuous monitoring for compliance with privacy laws and regulations. Implementation of this security control reduces the potential for unauthorized transfer of PII.	
REFERENCES	**RELATED CONTROLS**
Federal: 5 U.S.C. §552a(b); NIST SP: 800-37 Rev. 1 Appendix G; OMB Memo: M-06-19, M-07-16	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) the organization defines security policy filters to be used as a basis for enforcing flow control decisions; (ii) the organization defines information flows for which flow control decisions are to be applied and enforced; and (iii) the information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions for organization-defined information flows.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; information flow control policies; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; list of security policy filters regulating flow control decisions; information system audit records; and other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers. Test: Automated mechanisms implementing information flow enforcement policy.	

AC-04(12): DATA TYPE IDENTIFIERS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system, when transferring information between different security domains, uses HHS-defined data type identifiers to validate data essential for information flow decisions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Ensure that the minimum security controls identified in this overlay for PHI are in place to protect the data before transferring data between security domains. The confidentiality of PHI is better protected when a system can automatically detect data types and usage when being transferred from one security domain to another. This includes, for example, transfers between systems having different access controls with only a limited set of users allowed access to the PHI.	
REFERENCES	**RELATED CONTROLS**
Federal: 45 C.F.R. §164.312	
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if the information system uses HHS-defined data type identifiers to validate data essential for information flow decisions.
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing information flow; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records. Ensure that the system documentation describes: 1. The process for ensuring that each user receives only authorized data; 2. How the system processes all data traversing the network interface according to the applied access policy and/or filtering mechanism; and 3. Any requirements of boundary defense mechanisms at layered or internal enclave boundaries when security boundaries are traversed. Examine: Information system enforces approved authorizations for controlling the flow of information between security domains. Examine the information system security policy, system design documents, and documentation addressing information flow enforcement to confirm that: 1. The system assigns explicit HHS-defined data type identifiers on information, source, and destination objects; and 2. The system reviews the data type identifiers of all outgoing (i.e., going outside of the security domain) traffic (i.e., traversing the interconnected information system perimeter) based on associated HHS-defined data type identifiers (or data content where applicable) prior to release. Interview: Administration personnel knowledge of cross-domain information flow and interconnection processes and procedures. Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Confirm that information flow enforcement is properly implemented using HHS-defined data type identifiers as the basis for flow control decisions.

AC-04(15): DETECTION OF UNSANCTIONED INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system, when transferring information between different security domains, examines the information for the presence of unsanctioned information and prohibits the transfer of such information in accordance with the HHS information security and privacy policy.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
To provide the ability for an organization to monitor and prevent transfer of PII across different security domains, a system needs to have mechanisms to automatically detect, and where appropriate, prohibit the unauthorized transfer of PII across different security domains. Typical implementations of such controls will detect particular data types or metadata tagging and take action to prevent the transfer of the information beyond the intended boundaries. The organization ensures systems containing moderate and high PII confidentiality impact level information include the capability for the organization to centrally monitor for and detect unauthorized transfer of such PII across different security domains. Some technologies that would facilitate this include data-loss prevention, data-rights management, and key-word detection to prevent the unauthorized export of information from a network or to render such information unusable in the event of the unauthorized export of such information between security domains.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b), (e)(9)-(10); 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(5)(ii)(B)	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the information system examines the information for the presence of unsanctioned information and prohibits the transfer of such information.
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing information flow; system security plan; information system configuration settings and associated documentation; information system connection or processing

agreements; account management documents; other relevant documents or records. Verify system design documentation describes how unsanctioned information is detected and how transfer is prevented. Interview: Administration personnel's knowledge of cross-domain information flow and interconnection processes and procedures. Verify organization specifies sanctioning criteria or unsanctioned information or information types, or specifically specifies sanctioned information. Examine: Information system enforces restrictions on passing of unsanctioned data between security domains. Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Transmission of an unsanctioned information type is prevented from passing. Test a sample of automated mechanisms to confirm that information flow enforcement is properly implemented using the presence of unsanctioned information as the basis for flow control decisions. Test methods may include: - Attempt to send unsanctioned information to improper destinations (systems or users) based on presence of unsanctioned information; - Verify that the information system detects the impermissible flow, prevents it, audits the violation; and - Notify the appropriate personnel. Verification process should also be executed from a malicious user perspective, where possible.

AC-04(17): DOMAIN AUTHENTICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system uniquely identifies and authenticates source and destination points by organization, system, application, and/or individual for information transfer.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The ability to identify source and destination points for PII flow within information systems is necessary for attribution and compliance with need to know requirements. Implement a higher level of granularity for identification and authentication based on sensitivity of the PII. This is not to determine permissibility of the transfer but to enable an audit capability.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(c) and (e)(10); OMB Memo: M-06-16	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the information system uniquely identifies and authenticates source and destination points.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system implements unique identification and authentication functionality, based on organization, system, application, and/or individual, for all source and destination points during information transfer. Interview: Administration personnel's knowledge of information flow and interconnection processes and procedures. Confirm that designated personnel maintain a list of authorized source and destination points. Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Source and destination are verified before data transmission occurs. Test a sample of automated mechanisms to confirm that information flow enforcement is properly implemented using uniquely identified and authenticated source and destination points are the basis for flow control decisions. Test methods may include: 1. Attempt to send information to /from unauthenticated source and destination points (systems or users); 2. Verify that the information system detects the impermissible flow, prevents it, audits the violation and notifies the appropriate personnel. Examine: Access control policy; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records. Examine: Information system implements unique identification and authentication functionality, based on organization, system, application, and/or individual, for all source and destination points during information transfer. Interview: Administration personnel knowledge of information flow and interconnection processes and procedures. Confirm that designated personnel maintain a list of authorized source and destination points.	

Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Source and destination are verified before data transmission occurs. Test a sample of automated mechanisms to confirm that information flow enforcement is properly implemented using uniquely identified and authenticated source and destination points are the basis for flow control decisions. Test methods may include: 1. Attempt to send information to /from unauthenticated source and destination points (systems or users). 2. Verify that the information system detects the impermissible flow, prevents it, audits the violation, and notifies the appropriate personnel.

AC-04(18): SECURITY ATTRIBUTE BINDING

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system binds security attributes to information using CMS approved processes and procedures to facilitate information flow policy enforcement	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
To have a high level of trust in the information flow of sensitive information such as PII, this control ensures the security attributes selected in AC-16 are bound to the information. To ensure the protection of PII throughout its information flow, this control should be used to protect PII as it travels within and among information systems and information system components, such as database servers, application servers, shared storage environments, document repositories, and file folders.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-07-16, M-06-16; OMB Circular A-130: 7.g. w/Section 8 and Appendix III; 45 C.F.R. §164.306(a)	AC-16
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the information system binds security attributes to information.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing information flow; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records. Examine: Information system implements functionality that binds security attributes to information as part of the information flow enforcement. Examine method of binding security attributes to the information. Interview: Administration personnel knowledge of information flow and interconnection processes and procedures. Test: Automated mechanisms implementing information flow enforcement policy and mechanisms. Transmit information verifying security attributes are bound to data. Test a sample of automated mechanisms to confirm that information flow enforcement is properly implemented using security attributes attached to information as the basis for flow control decisions.	

AC-04(21): PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system separates information flows logically or physically using FedRAMP-approved mechanisms and/or techniques to accomplish required separations by types of information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system implements functionality that binds security attributes to information as part of the information flow enforcement. Test: Automated mechanisms implementing information flow enforcement functions.

AC-05: SEPARATION OF DUTIES

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Separates duties of individuals as necessary (defined in the applicable SSP), to prevent malicious activity without collusion; b. Documents separation of duties; and c. Defines information system access authorizations to support separation of duties.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E, CMS-ARS: Std.1 - Audit functions must not be performed by security personnel responsible for administering access control. Std.2 - Maintain a limited group of administrators with access based upon the users' roles and responsibilities. Std.3 - The critical mission functions and information system support functions must be divided among separate individuals. Std.4 - The information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions must be divided among separate individuals or groups. Std.5 - An independent entity, not the Information Owner(s)/Custodian(s), ISSO, System Developer(s)/Maintainer(s), or System administrator(s) responsible for the information system, conducts information security testing of the information system. **CMS-ARS**: High: Std.6 - The quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions must be conducted by an independent entity rather than the code developers. Moderate Cloud: Std.1 - For cloud service providers, the organization: a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies; b. Configures the information system to request user ID and authenticator prior to system access; and c. Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate. Std.2 - FedRAMP-defined subjects may explicitly be granted FedRAMP-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. Std.3 - AC-5 is not required at Low level for FedRAMP-authorized service providers.	
SUPPLEMENTAL GUIDANCE	
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Separation of duties aligns privileges with appropriate roles with the idea that duties are split between roles in such a way as to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this	

control helps reduce the risk of inappropriate access to sensitive information (e.g., separating employees that perform security investigations from mission and business functions).

HIPAA:
HIPAA requires the separation of duties to ensure that checks and balances are designed into the system to limit the effect of any given end user to control the entire process. Roles and responsibilities should be divided so that a single end user cannot subvert a critical process. This practice divides the tasks related to maintaining system security among different personnel such that no single individual could compromise PHI.

PII:
Separation of duties aligns privileges with appropriate roles with the idea that duties are split between roles in such a way as to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this control helps reduce the risk of inappropriate access to PII (e.g., separating employees that perform security investigations from mission and business functions).
Separation of duties is implemented by designating a selected set of administrators the capability to set user permissions to PII and PHI information, while those administrators do not themselves have access to the PII and PHI. The principle of separation of duties is significant for developers as well as for operational system administrators.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9)-(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-4, SD-1, SD-2; HIPAA: 45 C.F.R. §164.308(a)(3)(i), 164.308(a)(4)(i), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(c)(1); IRS1075; CJIS 5.6	AC-3, AC-6, PE-3, PE-4, PS-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing division of responsibility and separation of duties; information system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; list of user accounts and privileged accounts; information system audit records; and other relevant documents or records.
Examine: Verify that an access control mechanism resides on the information system that prevents users from having all of the necessary authority or information access to perform malicious activity without collusion.
Examine: Examine system configuration files to confirm that access authorizations have been set up properly for the various roles. Confirm that access control mechanism residing on the information system is configured to prevent users from having all of the necessary authority or information access to perform malicious activity without collusion.
Examine: Information system implements functionality that enforces separation of duties. Examples:
- RBACs and schema are defined and used;
- Privileged escalation mechanisms (tools) require authentication; and
- Shared accounts are not used.
Interview: Organizational personnel with responsibilities for defining appropriate division of responsibility and separation of duties. Confirm privileged users have limited duties.
Test: Automated mechanisms implementing separation of duties policy.

AC-06: LEAST PRIVILEGE

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with HHS missions and business functions.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Low Plus, Moderate, High:

Std.1 - Disable all file system access not explicitly required for system, application, and administrator functionality.
Std.2 - Contractors must be provided with minimal system and physical access, and must agree to and support the HHS security requirements. The contractor selection process must assess the contractor's ability to adhere to and support HHS security policy.
Std.3 - Restrict the use of database management utilities to only authorized database administrators.
Std.4 - Disable all system and removable media boot access unless it is explicitly authorized by the HHS CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected.

Moderate, High:
Std.5 - Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.
Std.6 - Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.

Web & Mobile:
Std.7 - Rights must be specifically added to an account to grant access to resources.
Std.8 - If rights are not explicitly necessary, then access should be denied.

SUPPLEMENTAL GUIDANCE

Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems.
The concept of least privilege aligns with the notion of only allowing access to sensitive information when a particular individual has a need-to-know in performance of their job duties.

PHI:
HIPAA requires least privilege to satisfy both the Minimum Necessary Rule and access control safeguards.

PII:
The concept of least privilege aligns with the notion of only allowing access to PII when a particular individual has a need-to-know in performance of their job duties.
The organization enforces the most restrictive set of rights/privileges or access needed by users (or processes acting on behalf of users) for the performance of specified tasks —increasing the level of restriction as PII confidentiality impact level rises.
The organization ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) necessary to perform their assigned tasks.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b), 45 C.F.R. §164.308(a)(4)(ii)(A), 45 C.F.R. §164.312(a)(1); HSPD 7: D(10); OMB Memo: M-06-16; IRS1075; CJIS 5.6	AC-2, AC-3, AC-5, CM-6, CM-7, PL-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Confirm that privileged accounts are created for users to perform privileged functions only; that is, privileged users use non-privileged accounts for all non-privileged functions. Review how least privilege is

determined for each user. Verify that each of the users actually has been granted the least privilege for the user's job in accordance with system documentation.
Examine: Information system implements functionality enforcing least privilege functions. Examples:
- RBACs and schema are defined and used;
- Privileged escalation mechanisms (tools) require authentication;
- No orphaned files (files not owned by a known system user) or files with uneven permissions (e.g., world has more access rights than the owner) exist on the system;
- Unexpected files and directories with excessive permissions (e.g., world write);
- Remote mounts/file shares minimize access granted;
- File protections minimize unauthorized access to sensitive files;
- Access by users to functionality is limited to functionality required for role/job;
- Access to privileged applications is limited;
- System accounts minimize access (e.g., not available for interactive use);
- Applications that are not configured to maximize security; and
- Unnecessary accounts have been removed.

Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. Confirm that the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.
Test: Automated mechanisms implementing least privilege functions [this is least functionality—different control]. Inspect system inventory to verify that only required applications are installed. Test a sample of the information system functions, particularly functions that require access for specific tasks by users and privileged users to confirm that the system has been configured with the most restrictive set of rights, privileges, or accesses possible and that users have been assigned the most restrictive set of rights, privileges, or accesses necessary. Verify that least privilege for the user has been assigned to the access of system resources.
The inventory of installed applications for deployed systems can be used to as an input to assess least privilege.

AC-06(01): AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information:
a. Setting/modifying audit logs and auditing behavior;
b. Setting/modifying boundary protection system rules;
c. Configuring/modifying access authorizations (i.e., permissions, privileges);
d. Setting/modifying authentication parameters; and
e. Setting/modifying system configurations and parameters.

IRS:
f. Explicitly authorize access to FTI

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - For cloud service providers, the organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.
Std.2 - For cloud service providers, the organization defines the list of security functions. The list of functions is approved and accepted by the Joint Authorization Board (JAB).

CMS-MARS:
Std.1 - The System Owner explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information for authorized personnel, including, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

SUPPLEMENTAL GUIDANCE

Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

PII:
Limiting access to security functions to authorized personnel reduces the number of users able to perform certain security functions, such as configuring access permissions, setting audit logs, performing system management functions. Examples of authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. These types of security functions can provide a level of access to PII, and capabilities to manipulate it, in ways that other users roles typically could not.
The organization identifies the security relevant functions that require authorized access for all information systems that contain moderate or high PII confidentiality impact level information.

REFERENCES	RELATED CONTROLS
Federal: Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.502(b) ; CJIS 5.6	AC-17, AC-18, AC-19

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing least privilege; list of security functions and security-relevant information for which access must be explicitly authorized; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Verify that the organization explicitly authorizes access to the control-specified list of security functions at a minimum(deployed in hardware, software, and firmware) and security-relevant information:
Examine: Information system implements functionality enforcing restrictions on access to security applications. Verify access to defined security functions and security information has been granted to specifically authorized personnel only.
Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks.
Test: Automated mechanisms forcing authorization prior to access to security functions.
The organization may also implement a solution that forces a user to go through an additional authorization before access to an elevated privilege is granted to security applications. (This may include privilege elevation applications such as sudo or the use of multiple accounts for users with access to elevated privileges.)

AC-06(02): NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization requires that users of information system accounts, or roles, with access to security functions or security-relevant information, use non-privileged accounts, or roles, when accessing non-security functions.

IRS:
The organization requires that users of information system accounts, or roles, with access to security functions, security-relevant information, or FTI use non-privileged accounts, or roles, when accessing non-security functions.

CMS-ARS, CMS-MARS-E:
At a minimum, the organization requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audit any use of privileged accounts, or roles, for such functions:
(i) Setting/modifying audit logs and auditing behavior
(ii) Setting/modifying boundary protection system rules
(iii) Configuring/modifying access authorizations (i.e., permissions, privileges)
(iv) Setting/modifying authentication parameters
(v) Setting/modifying system configurations and parameters.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS, CMS-MARS-E: CSP-1 - For cloud service providers, the organization requires that users of information system accounts, or roles, with access to all security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	
SUPPLEMENTAL GUIDANCE	
This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as RBAC and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.502(b); CJIS 5.6	PL-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements functionality enforcing use of non-privileged accounts/roles before being granted access to applications with elevated privileges. Confirm that procedures exist limiting performance of privileged functions to privileged accounts only, and that all non-privileged activities are relegated to non-privileged accounts. Verify that individual privileged users also have a non-privileged account. Examine: Examine the information system security configuration files and user accounts with parameters including assigned privileges to confirm that privileged accounts have been created for privileged users to perform privileged functions. Review the listing of privileged system user accounts. Identify the user accounts that have system privileges (e.g., system users who have the capability to perform system functions including change system configuration, reset security policy and settings, start/shut down system, perform system backup, data restore). Confirm that access to privileged accounts is limited to privileged users. Review detailed configuration and analyze for indications to the contrary that privileged accounts are created and used only for privileged functions. Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. Test: Automated mechanisms implementing least privilege functions. Confirm that security functions and security-relevant information cannot be accessed from a non-privileged account.	

AC-06(03): NETWORK ACCESS TO PRIVILEGED COMMANDS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization authorizes network access to privileged commands only for compelling operational needs as defined in the System Security Plan and documents the rationale for the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Examples include: - Setting/modifying audit logs and auditing behavior; - Setting/modifying boundary protection system rules; - Configuring/modifying access authorizations (i.e., permissions, privileges); - Setting/modifying authentication parameters; and - Setting/modifying system configurations and parameters.	
REFERENCES	**RELATED CONTROLS**

Federal: Code: 5 U.S.C. §552a(b)(1); OMB Memo: M-06-16	AC-17
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing least privilege; list of privileged commands assigned to information system accounts or roles; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements functionality restricting network access to privileged commands to only documented accounts/roles. Confirm that procedures exist limiting network-based performance of privileged functions to documented accounts/roles only. Confirm that the SSP documents a compelling operational need for any network-based privileged access. Examine: Examine the information system security configuration files and user accounts. Identify the user accounts that are allowed network-based access to privileged commands. For each identified account, confirm that network-based access to privileged commands is documented in the SSP. Interview: Organizational personnel with responsibilities for assigning network access to privileged commands. Interview: Organizational personnel granted network access to privileged commands. Test: Automated mechanisms implementing least privilege functions. Confirm that security functions and security-relevant information cannot be accessed from a non-privileged account.	

AC-06(05): PRIVILEGED ACCOUNTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization restricts privileged accounts on the information system to personnel with roles requiring privileged access and defined in the system security plan. **IRS:** Restrict privileged accounts on the information system to a limited number of individuals with a need to perform administrative duties	
CONTROL IMPLEMENTATION STANDARDS	
Std 1. Privileged users will use a separate non privileged account to perform internet browsing, email functions, word processing, etc.	
SUPPLEMENTAL GUIDANCE	
Privileged accounts, including super user accounts, are typically described as system administrator for various types of COTS operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. PII: This control limits who is authorized to administrative accounts, such as those who can perform security functions, which include configuring access permissions, setting audit logs and performing system management functions. These types of system and network management personnel typically have a level of access that is capable of circumventing other access controls. Limiting access to these accounts further protects sensitive information by limiting the number of individuals that have the “keys to the kingdom” on a network or system.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.308(a)(3)(i); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.312(a)(1); CJIS 5.6	CM-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Access control policy; system security plan; procedures addressing least privilege; list of system-generated super user accounts; list of system administration personnel; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Privileged accounts/roles on information systems are restricted to defined personnel. Examine configuration files to verify that access to privileged accounts has been granted to only organization-defined personnel. Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. Test: Automated mechanisms implementing least privilege functions. Automated mechanisms ensure only accounts with appropriate privileges can access privileged function.

AC-06(07): REVIEW OF USER PRIVILEGES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Reviews the privileges assigned to defined personnel or roles defined in the applicable SSP every 90 days to validate the need for such privileges; and b. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Review of user privileges is necessary in order to ensure privileges are revoked for those who no longer require access to sensitive information. Implementation of this control reduces the risk of unauthorized access to sensitive information by users who no longer need access to perform their job functions.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b) , (e)(9)-(10); OMB Memo: M-07-16; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.308(a)(4)(i); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. 45 C.F.R. §164.312(a)(2)(i); 45 C.F.R. §164.312(a)	CA-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every 90 days to validate the need for such privileges; and (ii) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing review of roles and personnel reassignment; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system implements functionality that assists in the periodic review of user privileges. Examine evidence of privileges review, such as meeting records, system change records. Interview: Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks. Test: Automated mechanisms implementing review of user privileges.	

AC-06(09): AUDITING USE OF PRIVILEGED FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, IRS, CJIS, VA
CONTROL REQUIREMENTS	
The information system audits the execution of privileged functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the Advanced Persistent Threat (APT). PII: Privileged functions have elevated permissions to access, and grant access, to sensitive information. Accountability requires the ability to detect, trace, and audit a privileged function whenever it is executed.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and Appendix III; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R.§164.312(b); CJIS 5.6	AU-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements functionality that audits the execution of privileged functions. Examine audit records for evidence of execution of privileged functions. Test: Automated mechanisms auditing the execution of least privilege functions. Automated mechanisms ensure accessing privileged functions appear in audit trails.	

AC-06(10): PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. PII: Non-privileged users may not have the same level of trust as privileged users. Privileged functions have access beyond that of the typical user, and as such may have greater ability to access sensitive information. Individual accountability requires the ability to trace (audit) the actions of the user who initiated them.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and Appendix III	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing Non-Privileged Users executing Privileged Functions; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.	

Examine: Information system implements functionality that prevents non-privileged users from executing privileged functions. Examine audit records, searching for attempts by non-privileged users to use privileged functions. Test: Automated mechanisms implementing least privilege functions for non-privileged users. Attempt to access a privileged function from a non-privileged account. Attempt to disable, circumvent and/or alter implemented safeguards/countermeasures. Attempt should fail.

AC-07: UNSUCCESSFUL LOGON ATTEMPTS

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and b. Automatically disables or locks the account/node until released by an administrator or after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. **IRS:** Specific to mobile device requirements, the logon is to the mobile device, not to any one account on the device. Additional mobile device controls are addressed in Section 9.3.1.14, Access Control for Mobile Devices (AC-19), and IRS 1075 Section 9.4.8, Mobile Devices.	
CONTROL IMPLEMENTATION STANDARDS	
Low, Low Plus: Std.1 - Configure the information system to lock out the user account automatically after five (5) consecutive invalid login attempts during a 15 minute time period. Require the lock out to persist for a minimum of fifteen (15) minutes. Moderate: Std.1 - Configure the information system to lock out the user account automatically after three (3) consecutive invalid login attempts during a 60 minute time period. Require the lock out to persist for a minimum of thirty (30) minutes. High: Std.1 - Configure the information system to lock out the user account automatically after three (3) consecutive invalid login attempts during a 120 minute time period. Require the lock out to persist until released by an administrator. **SPI:** The applicant/bidder locks the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store HHS Confidential Information. **IRS:** Std.1 - Configure the information system to lock out the user account automatically after three (3) consecutive invalid login attempts during a 120 minute time period. Require the lock out to persist for a minimum of fifteen (15) minutes. **CMS-ARS:** Cloud: Std.1 - For cloud service providers, the information system: a. Enforces a limit of not more than three (3) consecutive invalid login attempts by a user during a fifteen (15) minute time period; and b. Automatically locks the account/node for thirty (30) minutes when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection. **CMS-MARS-E:**	

Std.1 - The information system is configured to lock out the user accounts automatically after three (3) invalid login attempts through either a local or network connection during a fifteen (15)-minute time period. The lockout is required to persist for a minimum of thirty (30) minutes.
SUPPLEMENTAL GUIDANCE
This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; OMB M-16-04; IRS1075-Sep2016 9.3.1.7; CJIS 5.6	AC-2, AC-9, AC-14, IA-5

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing unsuccessful login attempts; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements functionality that limits number of consecutive invalid login attempts and automatically locks accounts. Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts. Test to confirm that the information system automatically enforces a limit of OpDiv-defined number of consecutive invalid access/logon attempts by a user at which point the information system automatically locks the user's account or node. Verify that once locked, a user account or node remains locked until a period of time has elapsed, or the account is released by an authorized administrator or other action occurs.

AC-07(02): PURGE/WIPE MOBILE DEVICES

Priority: P2	
Baseline(s):	Overlay(s): IRS
CONTROL REQUIREMENTS	
Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms.	

REFERENCES	RELATED CONTROLS
Federal: IRS1075	AC-19, MP-5, MP-6, SC-13

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing unsuccessful login attempts on mobile devices; information system design documentation; information system configuration settings and associated documentation; list of mobile devices to be purged/wiped after organization-defined consecutive, unsuccessful device logon attempts; list of purging/wiping requirements or techniques for mobile devices; information system audit records; other relevant documents or records.

Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms implementing access control policy for unsuccessful device logon attempts.

AC-08: SYSTEM USE NOTIFICATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, Health and Human Services Commission (HHS) standards and guidance. Refer to Control Implementation below for HHS Approved System Identification/Logon Banner. b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and the warning banner must be applied at the application, database, operating system, and network device levels for all HHS systems that receive, process, store, or transmit data. User agreement/acknowledgement is also required and can be achieved in many ways, such as: 1. Click to accept Or 2. Proceeding past this point constitutes acceptance of the above. c. For publicly accessible systems: 1. Displays system use information when appropriate, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. **IRS:** c. The warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI. 1. Display the approved warning banner before granting further access For sample warning banners approved by the Office of Safeguards, see Exhibit 8 of IRS 1075.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 -The warning banner, all in upper case, shall read: System Identification/Logon Banner – LONG VERSION (preferred): WARNING: THIS IS A TEXAS HEALTH AND HUMAN SERVICES INFORMATION RESOURCES SYSTEM THAT CONTAINS STATE AND/OR U.S. GOVERNMENT INFORMATION. BY USING THIS SYSTEM YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE NO RIGHT OF PRIVACY IN CONNECTION WITH YOUR USE OF THE SYSTEM OR YOUR ACCESS TO THE INFORMATION CONTAINED WITHIN IT. BY ACCESSING AND USING THIS SYSTEM YOU ARE CONSENTING TO THE MONITORING OF YOUR USE OF THE SYSTEM, AND TO SECURITY ASSESSMENT AND AUDITING ACTIVITIES THAT MAY BE USED FOR LAW ENFORCEMENT OR OTHER LEGALLY PERMISSIBLE PURPOSES. ANY UNAUTHORIZED USE OR ACCESS, OR ANY UNAUTHORIZED ATTEMPTS TO USE OR ACCESS, THIS SYSTEM MAY SUBJECT YOU TO DISCIPLINARY ACTION, SANCTIONS, CIVIL PENALTIES, OR CRIMINAL PROSECUTION TO THE EXTENT PERMITTED UNDER APPLICABLE LAW. System Identification/Logon Banner – Short VERSION (only when systems have space limitations): WARNING: THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. BY USING THIS SYSTEM YOU ACKNOWLEDGE AND AGREE THAT YOU HAVE NO RIGHT OF PRIVACY IN CONNECTION WITH YOUR USE OF THE SYSTEM OR YOUR ACCESS TO THE INFORMATION CONTAINED WITHIN IT. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES. **CMS-MARS-E** Std.2 - The System Owner determines elements of the environment that require the System Use Notification control.	

Std.3 - The System Owner determines how System Use Notification will be verified and provides appropriate periodicity of the check.
Std.4 - If not performed as part of a Configuration Baseline check, the organization has a documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider.

SUPPLEMENTAL GUIDANCE

The warning banner language has very important legal implications for CMS and its information system resources. Should content need to be added to this banner, submit the modified warning banner language to the HHS CIO for review and approval prior to implementation. If an information system has character limitations related to the warning banner display, the HHS CIO can provide an abbreviated warning banner version. If this banner is inconsistent with any directives, policies, regulations, or standards, notify the HHS CIO immediately. All information system computers and network devices under CMS control, prominently display the notice and consent banner immediately upon users' authentication to the system, including, but not limited to, web sites, web pages where substantial personal information from the public is collected, SFTP, SSH, or other services accessed.
System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

PII:
System use notification (e.g., logon banner) does not satisfy the requirement for Privacy Act Statements or Privacy Act system of records notice, when applicable; see TR-01 and TR-02. System use notifications are the primary, interactive vehicle for notifying system users prior to accessing a system of the organization's monitoring practices and reminding users that unauthorized use is both prohibited and subject to criminal and civil penalties.

The system use notification requires explicit action from the system user to acknowledge the notice before they can enter the system. While system use notices are principally intended to convey information regarding consent to monitor (and other security-relevant information), they may also be, in some instances, an appropriate means to remind system users that the system being accessed contains sensitive PII and requires due care (e.g., a logon banner on an employee management system).

HIPAA:
Note that System Use Notification **does not** satisfy the requirement for privacy notice under the HIPAA Privacy Rule.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(3) and (e)(4); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; Department of Health and Human Services (HHS): Policy for Monitoring Employee Use of HHS IT Resources; OMB Circular A-130: 7.g.; 45 C.F.R. §164.520(1)(i); IRS1075; CJIS 5.6	TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Assessment 1
Examine: Access control policy; privacy and security policies; system security plan; procedures addressing system use notification; documented approval of information system use notification messages or banners; information system notification messages; information system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; and other relevant documents or records.
Examine: Information system implements the required message or banner. All vectors for system access need to be evaluated. These include but are not limited to:
1. Console (text or GUI console);
2. Remote access (e.g., Remote Desktop Protocol [RDP], SSH); and
3. Window Manager

Test: Automated mechanisms implementing the access control policy for system use notification. Confirm that the system use notification message remains on the screen until the user takes explicit actions to logon to the information system.

AC-09: PREVIOUS LOGON (ACCESS) NOTIFICATION

Priority: P3	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
When supported by the underlying operating system, the information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control is applicable to logons to information systems via human user interfaces and logons to systems that occur in other types of architectures (e.g., service-oriented architectures).	
REFERENCES	**RELATED CONTROLS**
Federal: FISCAM: AC-1, AS-2; CJIS 5.6	AC-7, CA-7(1), PL-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing previous logon notification; information system configuration settings and associated documentation; information system notification messages; information system design documentation; other relevant documents or records. Examine: Information system implements the required notification. Test: Automated mechanisms implementing the access control policy for previous logon notification. Confirm that the information system, upon successful logon, displays the date and time of the last logon.	

AC-09(01): UNSUCCESSFUL LOGONS

Priority: P3	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
When supported by the underlying operating system, the information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Due to the possibility that an unauthorized person may have the ability to logon to a system or application using an authorized person's logon account, all systems and applicable applications will provide an automated method of notifying the authorized user of the last successful logon date and time, and a number of previously unsuccessful logon attempts. It is important that training include reporting procedures and responsibility for authorized users to report unauthorized logons and unauthorized attempts to logon.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing previous logon notification; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements the required notification.	

Test: Automated mechanisms implementing the access control policy for previous logon notification. Confirm that the information system, upon successful logon, displays the number of unsuccessful logon attempts since the last successful logon.

AC-10: CONCURRENT SESSION CONTROL

Priority: P3	
Baseline(s): High	Overlay(s): DIR, CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system limits the number of concurrent sessions for each system account to one (1) session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may define the maximum number of concurrent sessions for information system accounts globally, by account type (e.g., privileged user, non-privileged user, domain, specific application), by account, or a combination. For example, organizations may limit the number of concurrent sessions for system administrators or individuals working in particularly sensitive domains or mission-critical applications. This control addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. A session is defined as an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon. One user session is the time between starting the application and quitting. Some systems may require concurrent user sessions to function properly. However, based on the operational needs, automated mechanisms limit the number of concurrent user sessions. It is good practice to have management's approval for any system to have user concurrent sessions. Management should review the need for user concurrent sessions within every three hundred sixty-five (365) days.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing concurrent session control; information system design documentation; information system configuration settings and associated documentation; system security plan (SSP); and other relevant documents or records. Examine: Information system implements the required limits on concurrent sessions. Confirm that a requirement (if applicable) for more than one concurrent session is documented in the SSP. Test: Automated mechanisms implementing the access control policy for concurrent session control. Confirm that the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.	

AC-11: SESSION LOCK

Priority: P3	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity (for both remote and internal access connections) or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate, High:	

Std.1 - Period of inactivity must be no more than 15 minutes before session lock occurs for remote and mobile devices and requires user re-authentication. As agencies continue to migrate to laptops and docking stations making clients increasingly mobile, this is a logical extension of that requirement.

SPI:
The applicant/bidder locks the password after a certain number of failed attempts and after 15 minutes of user inactivity in all computing devices that access or store HHS Confidential Information.

SUPPLEMENTAL GUIDANCE

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.
This control protects sensitive information from unauthorized access when system users are away from their workstation. Since 2007, OMB has required session lock for remote and mobile devices, a standard which is neither technically nor financially burdensome. Based on risk, many agencies have adopted 15-minute session locks by policy as a best practice.

PII:
This control protects personally identifiable information (PII) from unauthorized access when system users are away from their workstation. Since 2007, OMB has required session lock for remote and mobile devices, a standard which is neither technically nor financially burdensome. Based on risk, many agencies have adopted 15-minute session locks by policy as a best practice.

HIPAA:
Under HIPAA, this is an addressable control.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.312(a)(2)(iii); OMB Memo: M-06-16, M-07-16; 45 C.F.R. §164.312(a)(1); IRS1075; CJIS 5.6	AC-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; system security plan; and other relevant documents or records.
Examine: Information system implements the required limits on inactivity functionality.
Test: Automated mechanisms implementing the access control policy for session lock. Confirm that the information system initiates a session lock after the organization-defined time period of inactivity and maintains the session lock until the user reestablishes access using established identification and authentication procedures. Confirm user can initiate session lock, and then unlock session using established identification and authentication procedures.

AC-11(01): PATTERN-HIDING DISPLAYS

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE	
Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images conveys sensitive information.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing session lock; display screen with session lock activated; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system implements inactive session concealment functionality. Test: Information system session lock mechanisms. Confirm that, when activated, the information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	

AC-12: SESSION TERMINATION

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system automatically terminates a user session after thirty (30) minutes of inactivity. **CMS-MARS-E:** The information system automatically terminates a user session after fifteen (15) minutes of inactivity	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std.1 - Avoid non-expiring session cookies and set a reasonable expiration time for idle sessions. This will help protect user sessions from misuse if the cookie is captured. Std.2 - New sessions should be generated each time a user is authenticated. Std.3 - Sessions should be destroyed when a user logs out.	
SUPPLEMENTAL GUIDANCE	
This control addresses the termination of user-initiated logical sessions in contrast to SC-10, which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. PHI: Under HIPAA, this is an addressable control. PII: The session termination control requires implementing functionality to prevent unauthorized use of an established user session. This control protects sensitive information from unauthorized access when system users have initiated a session.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** IRS1075	SC-10, SC-23
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated documentation; system security plan; and other relevant documents or records. Examine: Information system automatically terminates a user session after defined conditions or events occur (as defined in the system security plan). Examine system security plan (SSP) -defined events and functionality that requires session termination. Test: Automated mechanisms implementing the account control policy for session termination. Confirm defined events cause a session to be terminated.

AC-12(01): USER-INITIATED LOGOUTS / MESSAGE DISPLAYS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to CJIS information resources; and (b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.	
REFERENCES	**RELATED CONTROLS**
CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing session termination; user logout messages; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers. Test: Information system session lock mechanisms.	

AC-14: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication; **CMS-ARS, CMS-MARS-E:** c. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication.	
CONTROL IMPLEMENTATION STANDARDS	

IRS: Std. 1 - FTI may not be disclosed to individuals on the information system without identification and authentication
SUPPLEMENTAL GUIDANCE
This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. PHI: Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing PHI. Therefore, un- identified and un-authenticated users must not access PHI. PII: Individual accountability requires the ability to trace (audit) the actions of the user who initiated them when accessing personally identifiable information (PII). Therefore, un-identified and un-authenticated users must not access PII. **IRS:** Examples of access without identification and authentication would be instances in which the agency maintains a publicly accessible website for which no authentication is required.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b); FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; OMB Circular A-130: 7.g. and Appendix III; 45 C.F.R. §164.312(a)(2)(i); IRS1075	AC-2(9), CP-2, IA-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; system security plan; list of information system actions that can be performed without identification and authentication; information system audit records; and other relevant documents or records. Examine: Information system identifies specific user actions that can be performed on the information system without identification or authentication. Examples: - Access to files or services without authentication (anonymous access); and - Anonymous FTP. Interview: System/network administrators; organizational personnel with information security responsibilities. Confirm that they have followed the guidelines provided and to further confirm that the organization has documented the rationale for providing such access. Test: Automated mechanisms implementing the policy for user actions not requiring identification and authentication. Confirm that the system is configured to allow for specific actions that a user is permitted to perform without identification and authentication.

AC-16: SECURITY ATTRIBUTES

Priority: P1	
Baseline(s): High	Overlay(s): HIPAA, CMS-ARS
CONTROL REQUIREMENTS	

The organization:
a. Provides the means to associate HHS Information Security-defined security attributes having defined security attribute values with information in storage, in process, and/or in transmission;
b. Ensures that the security attribute associations are made and retained with the information;
c. Establishes the permitted HHS Information Security-defined security attributes for HHS information systems; and
d. Determines the permitted HHS Information Security-defined values or ranges for each of the established security attributes.

CONTROL IMPLEMENTATION STANDARDS

HIPAA:
Std.1 - The organization provides the means to associate a security attribute of "Contains PHI" for data structures that are known or plan to contain PHI having value of "yes" or "no" with information in storage, in process, and/or in transmission.

CMS-ARS:
Std.1 - The organization provides the means to associate the following with information in storage, in process, and/or in transmission:
a. A security attribute to demonstrate the user (subject) has completed privacy training in the last year; and
b. For data structures that are known or plan to contain personally identifiable information (PII), a security attribute of "Contains PII" [having] value of "yes" or "no."

SUPPLEMENTAL GUIDANCE

Information is represented internally within information systems using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as binding and is typically inclusive of setting the attribute value and the attribute type. Security attributes when bound to data/information, enables the enforcement of information security policies for access control and information flow control, either through organizational processes or information system functions or mechanisms. The content or assigned values of security attributes can directly affect the ability of individuals to access organizational information.

Organizations can define the types of attributes needed for selected information systems to support missions/business functions. There is potentially a wide range of values that can be assigned to any given security attribute. Release markings could include, for example, US only, NATO, or NOFORN (not releasable to foreign nationals). By specifying permitted attribute ranges and values, organizations can ensure that the security attribute values are meaningful and relevant. The term security labeling refers to the association of security attributes with subjects and objects represented by internal data structures within organizational information systems, to enable information system-based enforcement of information security policies. Security labels include, for example, access authorizations, data life cycle protection (i.e., encryption and data expiration), nationality, affiliation as contractor, and classification of information in accordance with legal and compliance requirements. The term security marking refers to the association of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies. The AC-16 base control represents the requirement for user-based attribute association (marking). The enhancements to AC-16 represent additional requirements, including information system-based attribute association (labeling). Types of attributes include, for example, classification level for objects and clearance (access authorization) level for subjects. An example of a value for both of these attribute types is Top Secret.

PII:
Implementation of this control provides a technical means to enforce security and privacy policies, e.g., access controls and encryption. Parameter values specified by the Privacy Overlays for this control include meta-data that supports privacy.
Using the security attributes listed in this control's parameter values section enables cross system functionality and reciprocity through consistent security attribute interpretation. This control supports privacy protections by assigning security attributes that characterize information, devices, or processes (i.e., an "object") as containing PII or associate an organization's mandatory security/privacy training requirement with a user (i.e., a "subject")

of an information system containing PII. The terms "Subject" and "Object" are defined in NIST SP 800-53, Rev. 4, Appendix B, Glossary.

Security attributes are meta-data about either a subject or an object. Other security attributes may exist for other requirements beyond privacy. If an organization creates security attributes it should be cognizant of the risk associated with including PII in that meta-data. However, PII is not included in the security attributes for the parameter values specified below.

HIPAA:
The parameter values for PHI enable policies, procedures, and data classification schemas that specify the application of administrative, technical, physical controls of a specific workstation or class of workstation that maintains electronic PHI.

REFERENCES	RELATED CONTROLS
Federal: Code: 5 U.S.C. §552a(b), (e)(9)-(10); FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.310(b); OMB Circular A-130: 7.g. and Appendix III	AC-2, AC-3, AC-4, AC-4(15), AC-4(18), AC-6, AC-21, AU-2, AU-10, SC-16, MP-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing the association of security attributes to information in storage, in process, and in transmission; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system implements required association of security attribute functionality.
Interview: System/network administrators; organizational personnel with information security responsibilities.
Test: Organizational capability supporting and maintaining the association of security attributes to information in storage, in process, and in transmission.

AC-16(03): MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM

Priority: P1

Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The information system maintains the association and integrity of the information attribute of "Contains PHI" to applicable information.

CMS-ARS:
The information system maintains the association and integrity of
a. The user attribute of "Annual PII Training" to individuals with access to personally identifiable information (PII); and
b. The information attribute of "Contains PII" to applicable information.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Implement policies, procedures, and data classification schemas that specify the manner in which the physical, technical, and security attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

CMS-ARS:
In an effort to use automated systems controls for PII and protected health information (PHI) objects, such as intrusion detection and key-word detection tools, maintaining the association and integrity of security attributes to subjects and objects can be used as the basis of automated policy actions.
Maintaining the association and integrity of security attributes to subjects and objects with sufficient assurance helps to ensure that the attribute associations can be used as the basis of automated policy actions. Automated policy actions include, for example, access control decisions or information flow control decisions.

REFERENCES	RELATED CONTROLS

Federal: Code: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130: 7.g. and Appendix III; 45 C.F.R. §164.310(b)	AC-4, AC-4(15), AC-4(18)

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization defines security attributes to be associated with organization-defined subjects and objects;
(ii) The organization defines subjects and objects requiring the association and integrity of security attributes to such subjects and objects to be maintained; and
(iii) The information system maintains the association and integrity of organization-defined security attributes to organization-defined subjects and objects.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing the association of security attributes to information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Interview: Organizational personnel with information security responsibilities; system developers.
Test: Automated mechanisms maintaining association and integrity of security attributes to information.

AC-17: REMOTE ACCESS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization monitors for unauthorized remote access to the information system (including access to internal networks by VPN). Remote access for privileged functions must be permitted only for compelling operational needs, must be strictly controlled, and must be explicitly authorized, in writing, by the HHS CIO or his/her designated representative.

If remote access is authorized, the organization:
a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

CMS-ARS:
c. Access to HHS Webmail using personally owned equipment is authorized. Access to other systems/networks using personally-owned equipment to a HHS CMS system is prohibited without written authorization from the HHS CIO, or an approved policy allowing the use of personally-owned equipment:
1. Personally-owned equipment must be scanned before being connected to HHS CMS systems or networks to ensure compliance with HHS requirements; and
2. Personally-owned equipment must be prohibited from processing, accessing, or storing Department sensitive information unless it is approved in writing by the HHS SOC and employs HHS required encryption (FIPS 140-2 validated module).

CONTROL IMPLEMENTATION STANDARDS

SPI:
Std.1 - The applicant/bidder secures, manages, and encrypt remote access (including wireless access) to computer systems containing HHS Confidential Information. (e.g., a formal process exists for granting access and validating the need for users to remotely access HHS Confidential Information, and remote access is limited to Authorized Users).

CMS-ARS:
Std.2 - Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor will be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems will be authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
Std.3 - All computers and devices, whether GFE, CFE, or personal, that require any network access to a HHS network or system are securely configured and meet, as a minimum, the following security requirements:
(a) Up-to-date system patches;

(b) Current anti-virus software;
(c) Host-based intrusion detection system;
(d) Functionality that provides the capability for automatic execution of code disabled; and
(e) Employs HHS required encryption (FIPS 140-2 validated module).
Std.4 - For organizations supporting remote access (including teleworking), ensure NIST SP 800-46 guidelines are followed by defining policies and procedures that define:
(a) Forms of permitted remote access;
(b) Types of devices permissible for remote access;
(c) Type of access remote users are granted; and
(d) How remote user account provisioning is handled.

CMS-MARS-E:
Std.1 - Require callback capability with re-authentication to verify connections from authorized locations when a secure data communication service network cannot be used.
Std.2 - All computers and devices, whether organization-furnished equipment or contractor-furnished equipment, that require any network access to a network or system are securely configured and meet at least the following requirements:
(i) up-to-date system patches,
(ii) current anti-virus software, and
(iii) functionality that provides the capability for automatic execution of code disabled.
Std.3 - Remoted connection for privileged functions must be performed using multi-factor authentication following *Electronic Authentication Guidelines for ACA Administering Entity Systems,* which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

SUPPLEMENTAL GUIDANCE

Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted VPNs to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs, does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3.

HIPAA:
Implement technical security measures to guard against unauthorized remote access to electronic PHI that is being transmitted over an electronic communications network.

CMS-ARS:
Limiting access to personally identifiable information (PII) from remote networks and/or restricting activities that can be conducted with PII remotely reduces the risk of intentional and unintentional disclosures of PII that may not exist on an internal network.
Allow remote access to PII only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(e)(1); NIST SP: 800-46, 800-77, 800-113, 800-114, 800-121; OMB Memo: M-06-16, M-07-16; CJIS 5.6	AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system implements established and documented usage restrictions: 1. Monitors for unauthorized remote access; 2. Remote access to privileged functions (functions w/elevated privileges) is controlled; 3. Remote access requires authentication; and 4. Applications, to include network protocols, used for remote access are configured to maximize security. Examine: Information system has been configured to restrict remote access to documented and approved ports and protocols. Examples: - Only authorized ports and protocols (e.g., SSHv2, Secure Network Management Protocol [SNMPv3]) are enabled; and - Encryption enforces use of FIPS 140-2 compliant modules and cyphers Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities. Test: Remote access management capability for the information system. Examples of conditions that typically violate this control: - Disallowed (insecure) protocols (e.g., Telnet, SSHv1, SNMPv1/v2, SSL v3.0) enabled; - Encryption using non-FIPS 140-2-compliant cryptographic algorithms or modules; - Liberal remote access (e.g., any remote user with a valid account); - Remote applications not configured to maximize security; and - Remote access protocols not enforcing re-authentication.

AC-17(01): AUTOMATED MONITORING / CONTROL

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system monitors and controls remote access methods.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: High & Moderate: Std.1 - The organization implements HHS and federally distributed blocking rules within one hour of receipt.	
SUPPLEMENTAL GUIDANCE	
Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Auditing remote access ensures unauthorized connections to information systems containing sensitive information can be detected across all information system platforms (e.g., servers, mobile devices, work stations). **CMS-ARS:** Auditing remote access ensures unauthorized connections to information systems containing personally identifiable information (PII) can be detected across all information system platforms (e.g., servers, mobile devices, work stations). Audit all remote access to, and actions on, resources containing PII.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-06-16, M-07-16, M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.310(b); 45 C.F.R. §164.310(c); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(e)(1); CJIS 5.6	AU-2, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system implements remote access monitoring and control functionality. Test: Automated mechanisms monitoring and controlling remote access methods.

AC-17(02): PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): SPI, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	
CONTROL IMPLEMENTATION STANDARDS	
SPI: Std.1 - The applicant/bidder secures, manages, and encrypt remote access (including wireless access) to computer systems containing HHS Confidential Information. (e.g., a formal process exists for granting access and validating the need for users to remotely access HHS Confidential Information, and remote access is limited to Authorized Users).	
SUPPLEMENTAL GUIDANCE	
The encryption strength of a mechanism is selected based on the security categorization of the information. Use only the HHS-approved encryption standard (see SC-13). **CMS-ARS:** Encrypting remote sessions protects the confidentiality and integrity of sensitive information. PHI: Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16, Step 3; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(e)(2)(ii); CJIS 5.6	SC-8, SC-12, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s). **CMS-ARS:** Determine if the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Test: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions. **CMS-ARS:** Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Examine: Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Test: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions.	

AC-17(03): MANAGED ACCESS CONTROL POINTS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system routes all remote accesses through a limited number of managed access control points. The organization must identify acceptable network access control points (e.g., connections standardized through the Trusted Internet Connections (TIC) initiative).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the TIC initiative requirements for external network connections.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	SC-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system limits remote access to defined, secure, and managed access points, ports, and protocols. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms routing all remote accesses through managed network access control points.	

AC-17(04): PRIVILEGED COMMANDS / ACCESS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and b. Documents the rationale for such access in the security plan for the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **Federal:** FedRAMP Rev. 4 Baseline	AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; system security plan; information system audit records; and other relevant documents or records. Examine: Information system restricts remote access to privileged commands and access to security-relevant information. Examine documented rationale for each user's or group's remote access to execute privileged commands. Test: Automated mechanisms implementing remote access management. Example: Disabling root access under *NIX sudo command.	

AC-17(06): PROTECTION OF INFORMATION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational need; and (b) Documents the rationale for such access in the security plan for the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing remote access to the information system; other relevant documents or records. Interview: Organizational personnel with responsibilities for implementing or monitoring remote access to the information system; information system users with knowledge of information about remote access mechanisms; organizational personnel with information security responsibilities.	

AC-17(09): DISCONNECT / DISABLE ACCESS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization provides the capability to expeditiously disconnect or disable remote access to the information system within one (1) hour.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The organization terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the HHS CIO, CISO, or Senior Official for Privacy (SOP). **CMS-ARS:** Moderate: CSP.1 - The organization terminates or suspends network connections with 15 minutes of direction by HHS.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing connection disconnect; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system provides the ability to disconnect or disable remote access within the required time period. Test: Automated mechanisms implementing remote access management.	

AC-18: WIRELESS ACCESS

Priority: P1

Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

If wireless access is authorized, the organization:
a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access;
b. Authorizes wireless access to the information system prior to allowing such connections;

CMS-MARS-E:
a. Prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the HHS CIO or a designated representative;
b. Monitors for unauthorized wireless access to information systems by employing a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system, and
c. Establishes for authorized wires access usage restrictions, configuration/connection requirements, and implementation guidance for wireless access prior to allowing such connections.

CMS-ARS:
c. The organization ensures that:
1.The HHS CIO must approve and distribute the overall wireless plan for his or her respective organization;
2. Organizations adhere to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN); and
3. Mobile and wireless devices, systems, and networks are not connected to wired HHS networks except through appropriate controls (e.g., VPN port) or unless specific authorization from HHS network management has been received.

IRS:
Additional requirements for protecting FTI on wireless networks are provided in Section 9.4.18, Wireless Networks

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The wireless policy shall address the following topic areas:
a. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.
b. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information. State organizations shall not transmit confidential information via a wireless connection to, or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards, are used to protect the information.
c. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without the approval of the state organization information resources manager.

CMS-ARS, CMS-MARS-E:
Std.2 - If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless restrictions and access controls are implemented:
a. Encryption protection is enabled;
b. Access points are placed in secure areas;
c. Access points are shut down when not in use (i.e., nights, weekends);
d. A stateful inspection firewall is implemented between the wireless network and the wired infrastructure;
e. MAC address authentication is utilized;
f. Static IP addresses, not DHCP, is utilized;
g. Personal firewalls are utilized on all wireless clients;
h. File sharing is disabled on all wireless clients;
i. Intrusion detection agents are deployed on the wireless side of the firewall;
j. Wireless activity is monitored and recorded, and the records are reviewed on a regular basis;
k. Adheres to HHS Policy for Wireless Client Access; and
l. Adheres to the HHS Standard for IEEE 802.11 Wireless Local Area Network (WLAN).
Std.3 - Wireless printers and all Bluetooth devices such as keyboards are not allowed.

CMS-MARS-E:
Std.2 -

m. Security Control SI-4(14), Employ a wireless intrusion "detection/prevention" system (WIDS/WIPS).	
SUPPLEMENTAL GUIDANCE	
Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., Extensible Authentication Protocol/Transport Layer Security [EAP/TLS], Protected Extensible Authentication Protocol [PEAP]), which provide credential protection and mutual authentication.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-1, AS-2; NIST SP: 800-48, 800-94, 800-97; IRS1075; CJIS 5.6	AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); activities related to wireless monitoring, authorization, and enforcement; information system audit records; and other relevant documents or records. Examine: Information system/network components monitor for unauthorized access, to include wireless, and detect/report the installation of wireless access points. 1. Use of wireless printers and Bluetooth devices is not allowed without explicit approval by the Authorizing Official (AO). Interview: Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system. Test: Wireless access management capability for the information system. A Network Access Control (NAC) capability is an example of a utility that can be deployed to detect the installation of a wireless access points. The NAC would be configured to deny access by default.	

AC-18(01): AUTHENTICATION AND ENCRYPTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
If wireless access is explicitly approved, the information system protects wireless access to the system using encryption, and authentication of both users and devices.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Communication over wireless networks, unless properly secured, has a greater risk of interception than hard-wired networks. Implementing encryption of wireless network communications containing personally identifiable information (PII) renders any intercepted data unreadable. If wireless networks permit access to organization information systems containing PII, then encryption of content and authentication of users or devices is required. Organizations should ensure that all WLAN components use FIPS-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-97, 800-153; CJIS 5.6	AC-3, IA-2, IA-3, IA-8, SC-8, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system protects wireless access to the system using encryption, and authentication of both users and devices. Examine encryption mechanism details to verify that encryption is performed by a FIPS 140-2-compliant cryptographic module operating in the FIPS-approved mode of operation. Interview: Organizational personnel responsible for authorizing, monitoring or controlling the use of wireless technologies in the information system. Test: Wireless access usage and restrictions. Automated mechanisms implementing the access control policy for wireless access to the information system.

AC-18(04): RESTRICT CONFIGURATIONS BY USERS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizational authorizations to allow selected users to configure wireless networking capability are enforced, in part by the access enforcement mechanisms employed within organizational information systems.	
REFERENCES	**RELATED CONTROLS**
	AC-3, SC-15
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system restricts the ability to configure wireless networking to designated users and/or roles. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms preventing independent configuration of wireless networking capabilities.	

AC-18(05): ANTENNAS / TRANSMISSION POWER LEVELS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) Reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) Employing measures such as TEMPEST to control wireless emanations; and (iii) Using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area.	
REFERENCES	**RELATED CONTROLS**

CJIS 5.6	PE-19

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Test: Automated mechanisms implementing the access control policy for wireless access to the information system; Wireless connections and access points outside of organizational boundaries using scanning devices.

AC-19: ACCESS CONTROL FOR MOBILE DEVICES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. HHS CIO authorizes the connection of mobile devices to organizational information systems.
c. The organization employs an approved method of cryptography (see SC-13) to protect Personally Identifiable Information (PII) residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops.

IRS:
Additional requirements on protecting FTI accessed by mobile devices are provided in Section 9.4.8, Mobile Devices.

CMS-MARS-E:
d. The organization monitors for unauthorized connections of mobile devices to information systems.
e. The organization enforces requirements for the connection of mobile devices to information systems.
f. The organization disables information system functionality that provides for automatic execution of code on mobile devices without user direction.
g. The organization issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
h. The organization protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code and virus protection software.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Encrypt information on all mobile devices that contains HHS Confidential Information.

CMS-ARS:
Cloud Moderate & Low:
CSP.1 - For cloud service providers, the organization defines inspection and preventative measures. The measures are approved and accepted by JAB.

CMS-MARS-E:
IS1. The organization defines inspection and preventive measures.
IS2. Purge/wipe information from mobile devices based on ten (10) consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones, and tablets). Laptop computers are excluded from this requirement.
IS3. Only organization-owned mobile devices and software can be used to process, access, and store PII.

SUPPLEMENTAL GUIDANCE

A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations.

Examples include smart phones, e-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The processing, storage, and transmission capability of the mobile device may be comparable to or merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled.

PII:
Limiting access to sensitive information from mobile devices reduces the risk of intentional and unintentional disclosures sensitive information PII that may not exist on an internal network.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** IRS1075; CJIS 5.6	AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system restricts/precludes access to interfaces and ports that support use of mobile devices.
Interview: Organizational personnel who monitor for unauthorized mobile device connections to CMS information systems.
Interview: Organizational personnel who use portable and mobile devices to access the information system.
Test: Automated mechanisms monitoring and implementing access control policy for portable and mobile devices.

AC-19(05): FULL DEVICE / CONTAINER-BASED ENCRYPTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

a. The organization employs HHS-required (FIPS 140-2 compliant module) full-device encryption to protect the confidentiality and integrity of information on approved HHS-controlled mobile devices.
b. The organization employs container encryption to protect the confidentiality and integrity of information on approved non HHS-controlled mobile devices.

CMS-ARS, CMS-MARS-E, IRS, CJIS:
a. The organization employs HHS-required (FIPS 140-2 validated module) full-device encryption or container encryption to protect the confidentiality and integrity of information on approved mobile devices.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - Encrypt information on all mobile devices that contain low, moderate, and high PII confidentiality impact level information.

CMS-MARS-E
Std.1 - For mobile devices containing Personally Identifiable Information (PII), employ encryption to protect the confidentiality and integrity of information on mobile devices (e.g., smartphones and laptop computers).

SUPPLEMENTAL GUIDANCE

Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including, for example, encrypting selected data structures such as files, records, or fields. FIPS 140-2 approved security function families are found at http://csrc.nist.gov/groups/STM/cavp/validation.html. However, implementing an approved security function is the start. The product must also be on the approved validation lists. (See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm for a list of current validated products.)

CMS-ARS:
Mobile devices are more likely to be lost or stolen and as a result sensitive information is more vulnerable. Encryption reduces this vulnerability.

PHI:
Under HIPAA, this is an addressable control.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16; 45 C.F.R. §164.312(a)(2)(iv); CJIS 5.6	MP-5, SC-13, SC-28

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing access control for mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Mobile device systems implement CMS required (FIPS 140-2 compliant module) functionality that provides full disk encryption or container encryption.
Test: Mechanisms implementing encryption control policy for mobile devices.
Full disk/device encryption applications must be configured to meet CMS requirements (FIPS 140-2 compliant module).

AC-20: USE OF EXTERNAL INFORMATION SYSTEMS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The HHS organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
a. Access the information system from external information systems; and;
b. Process, store, or transmit HHS-controlled information using the external information systems.

CMS-ARS:
Moderate, High:
The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the HHS CIO or his/her designated representative. If external information systems are authorized, the organization establishes strict terms and conditions for their use. The terms and conditions must address, at a minimum:

a. The types of applications that can be accessed from external information systems;
b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted;
c. How other users of the external information system will be prevented from accessing federal information;
d. The use of VPN and stateful inspection firewall technologies;

e. The use of and protection against the vulnerabilities of wireless technologies;
f. The maintenance of adequate physical security controls;
g. The use of virus and spyware protection software; and
h. How often the security capabilities of installed software are to be updated.

CMS-MARS-E
a. For organizational users (staff and contractors within the organization), the organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, such as Personally identifiable Information (PII), unless explicitly authorized, in writing, by the CIO or designated representative. If authorized, the organization establishes strict terms and conditions for their use.
b. For non-organizational users (such as business partners), the Administering Entity organization establishes terms and conditions, consistent with CMS implementation guidance of HHS Regulation 45 CFR 115.260, and in compliance with legal data sharing agreements signed with CMS, for any trust relationships established with other organizations owning, operating, and/or maintaining external information systems. These terms and conditions allow authorized individuals to:
b-1. The terms and conditions established for non-organizational users' use of external information systems allow authorized individuals to access the information system from external information systems
b-2. The terms and conditions established for non-organizational users' use of external information systems allow authorized individuals to process, store, or transmit organization-controlled information using external information systems.

IRS:
Unless approved by the Office of Safeguards, the agency must prohibit:
a. Access to FTI from external information systems, other than through a virtual desktop infrastructure (see Section 9.4.13 Virtual Desktop Infrastructure)

The agency may allow the use of personally-owned devices, without notification, only for the following purposes:
a. Bring Your Own Device (BYOD) used to access e-mail, where all requirements in Section 9.4.8 Mobile Devices are met
b. Remote access through a virtual desktop infrastructure (VDI) environment, where all requirements in Section 9.4.13 Virtual Desktop Infrastructure are met

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS, CMS-MARS-E:
Std.1 - Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls.
Std.2 - Limit remote access only to information resources required by home users to complete job duties.

CMS-MARS-E:
Std.3 - Only organization-owned computers and software can be used to process, access, and store Personally Identifiable Information (PII).

CMS-ARS:
Std.3 - Require that any government-owned equipment be used only for business purposes by authorized employees.

SUPPLEMENTAL GUIDANCE

External information systems are information systems or components of information systems that are outside of the authorization boundary established by organizations and for which organizations typically have no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. External information systems include, for example: (i) personally owned information systems/devices (e.g., notebook computers, smart phones, tablets, personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, train stations, convention centers, shopping malls, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of organizations. This control also addresses the use of external information systems for the processing, storage, or transmission of organizational information, including, for example, accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational information systems.

For some external information systems (i.e., information systems operated by other federal agencies, including organizations subordinate to those agencies), the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. Information systems within these organizations would not be considered external. These situations occur when, for example, there are pre-existing sharing/trust agreements (either implicit or explicit) established between federal agencies or organizations subordinate to those agencies, or when such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include, for example, organizational personnel, contractors, or other individuals with authorized access to organizational information systems and over which organizations have the authority to impose rules of behavior with regard to system access. Restrictions that organizations impose on authorized individuals need not be uniform, as those restrictions may vary depending upon the trust relationships between organizations. Therefore, organizations may choose to impose different security restrictions on contractors than on state, local, or tribal governments. This control does not apply to the use of external information systems to access public interfaces to organizational information systems (e.g., individuals accessing federal information through www.medicare.gov). Organizations establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum: types of applications that can be accessed on organizational information systems from external information systems; and the highest security category of information that can be processed, stored, or transmitted on external information systems. If terms and conditions with the owners of external information systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to HHS, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external.

PII:
Access to PII from external information systems (including, but not limited to, personally owned information systems/devices) is reinforced by a binding agreement to terms and conditions of the organization's privacy requirements to ensure awareness and accountability of both parties.
Such agreements may include memoranda of understanding (MOU), terms of service, or contracts.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FAR: Part 24, 39.105; FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AS-1, SM-7; OMB Circular A-130: 7.g.; 45 C.F.R. §164.312(a)(2)(i); IRS1075; CJIS 5.6	AC-1, AC-3, AC-17, AC-19, CA-3, PL-4, SA-9

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

CMS-ARS:
Determine if:
(v) Only organizational owned computers and software are used to process, access, and store PII.

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.
Test: Where authorized, external information systems connecting to the organization to store, access, transmit, or process sensitive information comply with HHS and organizational requirements.

AC-20(01): LIMITS ON AUTHORIZED USE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The HHS organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit HHS-controlled information only when the organization HHS: a. Verifies the implementation of required security controls on the external system as specified in the organization's HHS information security policy and security plan; or b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. PII: An external information system which processes, stores, or transmits sensitive information needs to have its security controls verified to meet the organization's security control requirements for information systems processing sensitive information.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(10); FAR: Part 24, 39.105; FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g.; 45 C.F.R. §164.314(a); CJIS 5.6	CA-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing the use of external information systems; system security plan; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Organization implements limitations on use of external information systems for external processing, storage, and transmission of organization-controlled information. Test: Automated mechanisms implementing limits on use of external information systems.	

AC-20(02): PORTABLE STORAGE DEVICES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization restricts the use of organization-controlled portable storage devices by authorized individuals on external information systems. **IRS:** Unless approved by the Office of Safeguards, the agency must prohibit the use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: IS1. Only organization-owned portable storage devices can be used to process, access, and store Personally Identifiable Information. These devices should employ encryption to protect the confidentiality and integrity of information.	
SUPPLEMENTAL GUIDANCE	

Limits on the use of organization controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing the use of external information systems; system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Organization restricts the use of organization-controlled portable storage devices on external information systems to authorized individuals. Examine list of users authorized to use portable storage on documented external information systems.	

AC-20(03): NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, IRS
CONTROL REQUIREMENTS	
The organization restricts the use of non-organizationally owned information systems, system components, or devices to process, store, or transmit organizational information. a. Use of contractor owned devices must be documented within the contract and the system security plan, employ information security and privacy protections appropriate for the sensitivity of the data, and be approved by the Authorizing Official (AO) in advance; and b. Use of personally owned devices must comply with HHS and CMS policies and directives on use of personally-owned information systems and components. **IRS:** a. Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation (see Section 7.4, 45-Day Notification Reporting Requirements)	
CONTROL IMPLEMENTATION STANDARDS	
High & Moderate: PRIV.1 - At a minimum controls must include implementation of either full-device or virtual container encryption to reduce the vulnerability of PII contained on mobile devices. PRIV.2 - Prior to being provided access to PII on remote devices, device users must acknowledge through a binding agreement their responsibilities to safeguard the PII accessible from the device and that they are aware of and agree to the organization's capabilities to manage the organization's PII on the device, including confiscation, in consultation with the organization's counsel, if necessary to remove the PII.	
SUPPLEMENTAL GUIDANCE	
Mobile devices are more vulnerable to loss or theft than other types of computing media (e.g., desktops and servers) due to their portability and widespread use inside and outside of government facilities. PII stored on mobile devices is more vulnerable as a result. This security control implements protections for PII contained on any mobile device not owned by the organization, including personal mobile devices, commonly referred to as BYOD. The organization should include in its mobile strategy a method to ensure both the device's access to PII can be revoked and the device's PII contents can be remotely removed.	
REFERENCES	**RELATED CONTROLS**
Code: 5 U.S.C. §552a(e)(10); HHS: IS2P 2014; OMB Memo: M-07-16, M-06-16	AC-19(5)
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Access control policy; system security plan; procedures addressing Bring Your Own Device (BYOD), security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; and other relevant documents or records. Examine: Information system restricts the use of portable storage devices. Interview: Organizational personnel with responsibilities for restricting or prohibiting use of non-organizationally owned information systems, system components, or devices; system/network administrators; organizational personnel with information security responsibilities; organizational personnel on use of BYOD. Test: Automated mechanisms implementing restrictions on the use of non-organizationally owned systems/components/devices.

AC-21: INFORMATION SHARING

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, CJIS, VA
CONTROL REQUIREMENTS	
The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for approved information-sharing circumstances where user discretion is required; and b. Employs HHS defined automated mechanisms, or manual processes, (defined in the applicable security plan) to assist users in making information sharing/collaboration decisions.	
CONTROL IMPLEMENTATION STANDARDS	
IRS: The agency must restrict the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards	
SUPPLEMENTAL GUIDANCE	
This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information (PII), classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. PHI: The HHS Senior Official for Privacy (SOP) may permit a business associate to create, receive, maintain, or transmit PHI on behalf of the organization to the extent the business associate is required by law to perform such function or activity, without meeting the requirements of a business associate contract, provided that the SOP attempts in good faith to obtain satisfactory assurances required in the business associate contracts, and documents the attempt and the reasons that these assurances cannot be obtained. This control helps covered entities to enforce the Minimum Necessary Rule. **CMS-ARS:** When PII is shared it is necessary to ensure the PII is being shared in accordance with statutory and regulatory requirements, including any restrictions on how the PII may be shared and the requirements for security of the receiving partner. This control addresses the sharing of information in a general sense (i.e., disclosure). It is not “information sharing” as defined by the Information Sharing Environment (ISE) Privacy Guidelines. All sharing partners, processes, and information systems must comply with applicable system of records notices (SORN), Privacy Impact Assessments (PIA), or other forms of notice or public statements. Examples of actions that may be required to implement privacy requirements in information sharing activities include: addressing privacy requirements in information sharing agreements; ensuring sharing partners have a mutual understanding of the PII confidentiality impact level (as NIST SP 800-122 is a risk based analysis and accepts variation in organizational implementation); developing processes and supporting mechanisms to ensure/enforce compliance; and implementing technical capabilities that enforce privacy requirements for PII stored or processed by a sharing partner. Program managers and system owners should work with their privacy offices to ensure information sharing activities are compliant with privacy requirements.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy	AC-3, TR-01, UL-02

State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b) and (e); FedRAMP Rev. 4 Baseline; Privacy: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment; 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(4)(ii)(B); 45 C.F.R. §164.308(a)(4)(ii)(C); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.314(a); IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing user-based collaboration and information sharing (including restrictions); information system design documentation; information system configuration settings and associated documentation; list of users authorized to make information sharing/collaboration decisions; list of information sharing circumstances requiring user discretion; and other relevant documents or records.
Examine: Information system restricts sharing of identified information to authorized users/roles.
Interview: Organizational personnel responsible for making information sharing/collaboration decisions.
Test: Automated mechanisms or manual process implementing access authorizations supporting information sharing/user collaboration decisions.

AC-22: PUBLICLY ACCESSIBLE CONTENT

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information monthly and removes such information, if discovered.

CMS-ARS, CMS-MARS-E:
d. Reviews the content on the publicly accessible information system for nonpublic information bi-weekly and removes such information, if discovered.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

In accordance with federal laws, Executive Orders, directives, policies, regulations, standards, and/or guidance, the general public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act and proprietary information). This control addresses information systems that are controlled by the organization and accessible to the general public, typically without identification or authentication. The posting of information on non-HHS information systems is covered by organizational policy.

PII:
Personally identifiable information (PII) that is maintained in a system of records or not approved for release under the Freedom of Information Act (FOIA) is nonpublic information. When agencies consider sharing or posting PII, they must do so in a way that fully protects individual privacy. Under HIPAA, a covered entity or business associate may not use or disclose protected health information except as provided by the HIPAA Privacy Rule. This control implements procedures to protect information, including PII, from being posted publicly improperly.
PII that is nonpublic information must not be posted onto a publicly accessible information system.

REFERENCES	**RELATED CONTROLS**

Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552(b)(6); FedRAMP Rev. 4 Baseline; OMB Memo: M-11-02; 45 C.F.R. §164.502(a); IRS1075; CJIS 5.6	AC-3, AC-4, AT-2, AT-3, AU-13

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; system security plan; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational information systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs; security awareness training records; other relevant documents or records.
Examine: Information system restricts sharing of identified information to authorized users/roles.
Interview: Organizational personnel responsible for managing publicly accessible information posted on organizational information systems.
Test: Automated mechanisms implementing management of publicly accessible content.

AC-23: DATA MINING PROTECTION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization employs methods for email or data files containing criminal justice information (CJI) to adequately detect and protect against data mining.

CONTROL IMPLEMENTATION STANDARDS

The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

SUPPLEMENTAL GUIDANCE

Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.

REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Access control policy; procedures addressing data mining techniques; procedures addressing protection of data storage objects against data mining; information system design documentation; information system configuration settings and associated documentation; information system audit logs; information system audit records; other relevant documents or records.
Interview: Organizational personnel with responsibilities for implementing data mining detection and prevention techniques for data storage objects; organizational personnel with information security responsibilities; system developers.
Test: Automated mechanisms implementing data mining prevention and detection.

(AT) AWARENESS AND TRAINING

The HHS organization(i) requires that users of HHS information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of HHS information systems; and (ii) requires that HHS personnel are complying with Agency security awareness training requirements.

AT-01: SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to personnel/roles as designated by the organization: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and, if necessary, updates the current: 1. Security awareness and training policy at least once every three (3) years (or if there is significant change); and 2. Security awareness and training procedures at least once every three hundred sixty five (365) days. **CMS-MARS-E:** b.1. Security awareness and training policy at least once every three hundred sixty five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency head or his/her designated representative(s) shall ensure that the agency has trained personnel to assist the agency in complying with the requirements of TAC 202 and related policies **CMS-MARS-E:** Std.2. The organization develops, documents, implements, disseminates to applicable personnel, and reviews and updates (as necessary), within every three hundred sixty-five (365) days a security and privacy awareness and training plan that addresses all requirements of the security and privacy training program. This plan should cover required policies and procedures and a documented process for implementing basic privacy and awareness training for all organizational users and contractors that includes understanding potential indicators of insider threats. This plan should also include requirements for ensuring personnel with specific roles and responsibilities in information security and privacy undergo more detailed and audience specific security and privacy training.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PII: Information security awareness and training complements privacy awareness and training efforts, particularly where the two disciplines overlap in the areas of use, confidentiality, access, integrity and protection of sensitive information. Coordination between the information security and privacy office on the proper use and protections to be afforded to personally identifiable information (PII) within security awareness and training policies addresses the purpose, roles and responsibilities surrounding PII compliance.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC 202.20(4)**,** DIR Security Control Standards Catalog	AR-5, AR-6, PM-9

Federal: Code: 5 U.S.C. §552a(e)(9)-(10), Public Law (PL) No. 107-347, §208; Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3, SM-4; HIPAA: 45 C.F.R. §164.308(a)(5)(i), 45 C.F.R. §164.308(a)(5)(ii)(A), 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-12, 800-16, 800-50, 800-100; OMB Memo: M-03-22, M-07-16; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security and privacy awareness and training policy and procedures, personnel training records; and other relevant documents.
Interview: Organizational personnel with information security and privacy awareness and training responsibilities, verify that required training is acknowledged. AT-2 Security Awareness Training (High, Moderate, Low) (PII, PHI) (CSP: Mod, Low) Assurance P1

AT-02: SECURITY AWARENESS TRAINING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users;
b. When required by system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

CMS-ARS, CMS-MARS-E, CJIS:
a. As part of initial training for new users prior to accessing any system's information;

CONTROL IMPLEMENTATION STANDARDS

High, Moderate, Low Plus & Low:
Std.1 - An information security and privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of HHS involved in managing, using, and/or operating information systems.
Std.2 - Information security and privacy education and awareness training must include responsibilities associated with sending sensitive information in email.
Std.3 - Privacy awareness training must be provided before granting access to HHS systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors, to explain the importance and responsibility in safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance.

CMS-ARS:
Moderate, High:
Std.4 - Provide privacy training for all systems with PII, commensurate with the PII confidentiality impact level. Integrate privacy training with general IA training.

High:
Std.5 - Provide privacy training for all systems with PII, commensurate with the PII confidentiality impact level. Integrate privacy training with general Information Assurance (IA) training.

IRS:
This section is closely coupled with Section 6.3, Disclosure Awareness Training, which provides the requirement for general FTI disclosure awareness training; however, this control is focused on information security and operational security awareness.

SUPPLEMENTAL GUIDANCE

Organizations determine the appropriate content of security and privacy awareness training, and security and privacy awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information

security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy as it relates to HHS's information security program. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events.

PHI:
The following elements of security training are addressable under HIPAA. Security Awareness Training should include:
(i) periodic security updates;
(ii) procedures for guarding against, detecting, and reporting malicious software;
(iii) procedures for monitoring log-in attempts and reporting discrepancies; and
(iv) procedures for creating, changing, and safeguarding passwords.

PII:
Information security awareness and training complements privacy awareness and training efforts, particularly where the two disciplines overlap in the areas of use, confidentiality, access, and integrity.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy, Security and Privacy Inquiry (SPI) **State:** TAC 202.24(b)(2-3); TGC 2054.134(d); DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(5)(ii); NIST SP: 800-50; OMB Memo: M-03-22, M-07-16; IRS1075; CJIS 5.6	AR-5, AR-6, AT-3, AT-4, PL-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security and privacy awareness and training policy, procedures addressing information security and privacy awareness training implementation, appropriate codes of federal regulations, information security and privacy awareness training curriculum, information security and privacy awareness training materials, system security plan, personnel training records, training logs, and other relevant documents or records.
Examine: Organization implements automated information security and privacy awareness training.
Interview: Organizational personnel comprising the general information system user community.
Test: Automated mechanisms managing information security and privacy awareness training.

AT-02(02): INSIDER THREAT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, MARS-E, VA

CONTROL REQUIREMENTS

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat, such as:
a. Inordinate, long-term job dissatisfaction,
b. Attempts to gain access to information not required for job performance,
c. Unexplained access to financial resources,
d. Bullying or sexual harassment of fellow employees,
e. Workplace violence, and
f. Other serious violations of organizational policies, procedures, directives, rules, or practices.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

IRS: Insider threat training should bring awareness of the potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform malicious actions, which could include the unauthorized access or re-disclosure of FTI.
SUPPLEMENTAL GUIDANCE
Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	PL-4, PM-12, PS-3, PS-6

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information security and privacy awareness and training policy; procedures addressing information security and privacy awareness training implementation; appropriate codes of federal regulations; information security and privacy awareness training curriculum; information security and privacy awareness training materials; system security plan; personnel training records; and other relevant documents or records. Interview: Organizational personnel comprising the general information system user community.

AT-03: ROLE-BASED SECURITY TRAINING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization provides role-based security training to personnel (both contractor and employee) with assigned information security and privacy roles and responsibilities (i.e., significant information security and privacy responsibilities): a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. Within every 365 days thereafter. **CMS-ARS:** c. Within sixty (60) days of entering a position that requires role-specific training, and within every 365 days thereafter.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS, CMS-MARS-E: Std.1 - Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to HHS networks, systems, and/or applications; when required by significant information system or system environment changes; and when an employee enters a new position that requires additional role-specific training and refresher training within every three hundred sixty-five (365) days thereafter. **CMS-ARS:** Std.2 - The minimal role-based security and privacy training received over a 365 day cycle must meet or exceed State/Federal minimal requirements as described in the HHS role-based training (RBT) policy. Std.3 - Information Security and Privacy awareness and training may be provided by the Agency or received by means of HHS-approved RBT courses, professional development, certificate programs, and/or traditional college credit courses. Std.4 - All HHS employees and contractors with significant information security roles and responsibilities that have not completed the required training within the mandated timeframes shall have their user accounts disabled until they have met their RBT requirement.	

PII:
High & Moderate:
PRIV.1 - Provide role-based privacy training for all systems with PII, commensurate with the PII confidentiality impact level.

CSP:
Moderate & Low:
CSP.1 - For cloud service providers, the organization provides information security and privacy refresher training a least every three (3) years thereafter.

IRS:
Personnel with security roles and responsibilities include, but are not limited to, the following positions: Information System Security Manager, Information System Security Officer, Security Specialist, Network Administrator, Systems Administrator, Database Administrator, Programmer/Systems Analyst, System Owner, Systems Designer/Systems Developer, helpdesk.

Note: Training conducted under this section is distinct from Section 6.3, Disclosure Awareness, and Section 9.3.2.2, Security Awareness Training (AT-2).

SUPPLEMENTAL GUIDANCE

Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of HHS and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of HHS's information security programs. Role-based security training also applies to contractors providing services to federal agencies.

PII:
Significant information security and privacy responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security and/or privacy posture of one or more CMS systems.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities; HIPAA: 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(i); NIST SP: 800-16, 800-50; OMB Memo: M-03-22, M-07-16; IRS1075; CJIS 5.6	AR-5, AR-6, AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security and privacy awareness and training policy; procedures addressing information security and privacy training implementation; codes of federal regulations; security training curriculum; information security and privacy training materials; system security plan; personnel training records; and other relevant documents or records.
Examine: Organization implements automated information security and privacy role-based training within required time frame.

Test: Automated mechanisms managing role-based information security and privacy training.

AT-04: SECURITY TRAINING RECORDS

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Documents and monitors individual information system security and privacy training activities, including basic security and privacy awareness training and specific role-based information system security and privacy training; and b. Retains individual training records for a minimum of five (5) years after completing a specific training course. **CMS-ARS:** c. Identifies employees and contractors who hold the roles with significant information security and privacy responsibilities	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Procedures and training implementation should: a. Identify employees with significant information security and privacy responsibilities and provide role-specific training in accordance with NIST standards and guidance: 1. All users of HHS information systems must be exposed to security and privacy awareness materials at least every 365 days. Users of HHS information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to HHS information systems and applications; 2. Executives must receive training in information security and privacy basics and policy level training in security and privacy planning and management; 3. Program and functional managers must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/ application life cycle management, risk management, and contingency planning; 4. CIOs, information security and privacy program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security and privacy officers) must receive training in information security and privacy basics and broad training in security and privacy planning, system and application security and privacy management, system/application life cycle management, risk management, and contingency planning; and 5. IT function management and operations personnel must receive training in information security and privacy basics; management and implementation level training in security and privacy planning and system/application security and privacy management; and management and implementation level training in system/application life cycle management, risk management, and contingency planning. b. Provide the HHS information systems security awareness material/exposure outlined in NIST guidance on information security awareness and training to all new employees before allowing them access to the systems; c. Provide information systems security and privacy refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees use or process; and d. Provide training whenever there is a significant change in the information system environment or procedures or when an employee enters a new position that requires additional role-specific training. Documentation for specialized training may be maintained by individual supervisors at the option of the organization. PII: Maintaining security training records provides the capability for organizations to track compliance with privacy-related training requirements. Under HIPAA, a covered entity must document that the training as described within the regulation has been provided as required.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9)-(10), Pub. L. No. 107-347, §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R.	AR-5, AR-6, AT-2, AT-3, PM-14

§164.308(a)(5)(i); 45 C.F.R. §164.308(a)(5)(i); 45 C.F.R. §164.530(b)(2)(ii) US HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities OMB Memo: M-03-22, M-07-16; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security and privacy awareness and training policy; procedures addressing Information security and privacy training records; Information security and privacy awareness and training records for personnel; and other relevant documents or records.
Examine: Organization implements automated required information security and privacy training records management.
Interview: Organizational personnel with Information security and privacy training record retention responsibilities.
Test: Automated mechanisms supporting management of Information security and privacy training records.

(AU) AUDIT AND ACCOUNTABILITY

The HHS organization (i) requires the creation, protection, and retention of information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) requires that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

AU-01: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates (as necessary) the current:
1. Audit and accountability policy at least every three (3) years; and
2. Audit and accountability procedures at least once every three hundred sixty five (365) days.

CMS-MARS-E:
b.1. Audit and accountability policy within every three hundred sixty-five (365) days

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
PRIV.1 - Review and update (as necessary) the current audit and accountability policy in accordance with organizational policy but not less than every 365 days.

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PII:

Security audit and accountability policies and procedures directly support privacy audit and accountability procedures.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); NIST SP: 800-12, 800-100; OMB M-07-16, Circular A-130, 7.g., and 8.b(2)(c); IRS1075	AU-2 , AR-4, PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy and procedures; other relevant documents or records. Interview: Organizational personnel with audit and accountability responsibilities.	

AU-02: AUDIT EVENTS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Determines that the information system is capable of auditing the events specified in Implementation Standard 4; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate (relevant) to support after-the-fact investigations of security and privacy incidents; and d. Determines which events are to be audited within the information system as defined in Implementation Standard 5.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Information systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or affect the release of confidential information. Std.2 - Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules. Std.3 - Based on the risk assessment, a sufficiently complete history of transactions shall be maintained to permit an audit of the information resources system by logging and tracing the activities of individuals through the system. Std.4 – The information system must have the capability to audit events stipulated as mandatory by the HHS CISO in the IS-Security Audit procedure. The information owner, based on a risk assessment and mission and business needs, may audit additional events outlined as optional in the IS-Security Audit procedure. The System Security Plan must document all auditable events the information system capable of auditing, which events are audited, and the frequency which the events are audited. Std.5 – The information system is required to audit all events mandated as required by the HHS CISO per the IS-Security Audit procedure at the frequency stipulated in the procedure.	
SUPPLEMENTAL GUIDANCE	
An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on	

system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. PII: This control identifies privacy-relevant security auditable events using a risk-based approach. Examples of privacy-relevant auditable events include logging access to or modification of PII. The parameter values for this control do not provide an exhaustive list of all auditable events, but instead list the auditable events required by OMB privacy policy. The organization should manage the length of time that a log file is maintained to the period necessary to comply with the organization's security and privacy policies.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b), 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R; NIST SP: 800-37, 800-39, 800-92, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04, M-06-16, M-07-16; OMB Circular A-130, 7.g., 8.b(2)(c)(iii) and Appendix I; Web: csrc.nist.gov/pcig/cig.html; IRS1075; CJIS 5.6	AC-6, AC-17, AR-4, AU-3, AU-12, MA-4, MP-2, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing auditable events; system security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records. Examine: Information system implements defined auditing functionality. Examples: - Auditing capability is installed, configured, and enabled; - System is configured to capture information on network activity that cannot be attributed to a user or service; - System and event logs are being collected as required and in the locations required; and - Privileged applications are configured to capture system and event logs. Interview: Organizational personnel with auditing and accountability responsibilities. Test: Automated mechanisms implementing information system auditing of organization-defined auditable events. Examine audit trail data to ensure list of events defined under implementation standards are collected.	

AU-02(03): REVIEWS AND UPDATES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization reviews and updates the list of auditable events no less often than every three hundred sixty-five (365) days and whenever there is a significant system modification.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The organization reviews and updates the list of auditable events as per the frequency defined in this control or whenever there is a change in the threat environment.	
SUPPLEMENTAL GUIDANCE	
Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.	
REFERENCES	**RELATED CONTROLS**
FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing auditable events; system security plan; list of organization-defined auditable events; auditable events review and update records; information system audit records; information system incident reports; and other relevant documents or records. Examine: Information system implements an update mechanism (automated or manual) for auditable events. Interview: Organizational personnel with auditing and accountability responsibilities. Test: Automated mechanisms supporting review and update of auditable events.

AU-03: CONTENT OF AUDIT RECORDS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system generates audit records containing information that specifies the requirement in implementation standard 1.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Required Contents of Audit Records: (a) Type of event; (b) Date and time of the event; (c) Component of the information system (e.g., software component, hardware component) where the event occurred; (d) Source of the event (e) Outcome (success or failure) of the event; and (f) User/subject identity associated with the event; **CMS-ARS:** (g) Execution of privileged functions. **HIPAA:** Std.2 - Record disclosures of sensitive information, including protected health and financial information	
SUPPLEMENTAL GUIDANCE	
Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). PII: Audit records that are commensurate with the privacy risk they address are an effective tool for identifying whether, when, and how issues have occurred related to data quality and privacy breaches.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST SP 800-92; FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); OMB Memo: M-06-16, M-07-16 Att. 1 OMB Circular A-130: 7.g., and 8.b(2)(c)(iii); IRS1075; CJIS 5.6	AR-4, AU-2, AU-8, AU-12, SI-11
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; and other relevant documents or records. Examine: Information system generates audit records containing required information. Examples: - Auditing is enabled and active; - Audit records contain the required information; and - Applications, including network protocols, are configured to capture required information. Test: Automated mechanisms implementing information system auditing of auditable events.

AU-03(01): ADDITIONAL AUDIT INFORMATION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
a. The information system generates audit records containing the following additional, more detailed information: - Filename accessed; - Program or command used to initiate the event; and - Source and destination addresses.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The information system includes (a) Additional more detailed session connection, transaction, and/or activity duration information. (b) The number of bytes received and bytes sent for client-server transactions. (c) Additional informational messages to diagnose or identify the event. The information system includes characteristics that describe or identify the object or resource acted upon in the audit records for audit events identified by type, location, or subject. Std.2 - The organization defines audit record types. The audit record types are approved and accepted by the System Owner.	
SUPPLEMENTAL GUIDANCE	
Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system design documentation; system security plan; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system generates audit records containing required additional information. Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject.	

AU-03(02): CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system provides centralized management and configuration of the content to be captured in audit records generated by individual components throughout the information system.	
CONTROL IMPLEMENTATION STANDARDS	
High, CMS-ARS Moderate & High: Std.1 - Centralized audit repositories must be searchable by HHS Information Security:	

(a) Information is available to HHS Information Security in a format compliant with HHS, State, CMS and Federal requirements; and (b) Centralized audit repository record sources include systems, appliances, devices, services, and applications (including databases). Std.2 - Raw audit records must be available in an unaltered format to HHS Information Security.
SUPPLEMENTAL GUIDANCE
This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Audit records contain evidence that can be used in the investigation of compromised systems. To prevent this evidence from being compromised, it must be sent to a separate system continuously. Methods for sending audit records include, but are not limited to, system audit tools used to send logs directly to another host or through the system's syslog service to another host.

REFERENCES	RELATED CONTROLS
Federal: NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	AU-6, AU-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Examine: Information system provides centralized management and configuration of the content to be captured. Examples: 1. Audit data is collected and analyzed centrally within the organization; and 2. Audit data is available to HHS Information Security for analysis. Test: Automated mechanisms implementing centralized management of audit record content.

AU-04: AUDIT STORAGE CAPACITY

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS
The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
CONTROL IMPLEMENTATION STANDARDS
Std.1 - Capacity must be sufficient to handle auditing records during peak performance times. **IRS:** Std.2 - The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years
SUPPLEMENTAL GUIDANCE
The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage PII: Adequate storage capacity for logs used to audit security- and privacy-related controls reduces the likelihood of the logs exceeding available storage space and potentially losing log information or reducing auditing capability. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act, and providing adequate storage capacity allows for preserving complete audit information for these purposes.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	AR-4, AU-2, AU-5, AU-5(1), AU-6, AU-7, AU-9, AU-9(2), AU-11, SI-4

Federal: Code: 5 U.S.C. §552a(i); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 164.312(b); OMB Memo: M-07-16; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(ii)(D); IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components that store audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system provides an appropriate storage capacity.
Interview: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. Discuss auditing during peak system operation.
Test: Audit record storage capacity and related configuration settings.

AU-05: RESPONSE TO AUDIT PROCESSING FAILURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system:
a. Alerts defined personnel or roles (defined in the applicable system security plan) in the event of an audit processing failure; and
b. Takes the actions defined in Implementation Standard 1 in response to an audit failure or audit storage capacity issue.

IRS:
c. Monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator

CONTROL IMPLEMENTATION STANDARDS

Low, Low Plus, Moderate:
Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system or halt processing;
(b) Stop generating audit records; or
(c) Overwrite the oldest records, in the case that storage media is unavailable.

High:
Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system or halt processing immediately; and
(b) Systems that do not support automatic shutdown must be shut down within 1 hour of the audit processing failure.

CMS-ARS:
Moderate:
Std.1 - Takes the following actions in response to an audit failure or audit storage capacity issue:
(a) Shutdown the information system or halt processing immediately; and
(b) Systems that do not support automatic shutdown must be shut down within 1 hour of the audit processing failure.

Cloud Moderate & Low:
CSP.1 - For MODERATE system cloud service providers, the information system takes the following actions in the event of an audit processing failure: Shut down.
CSP.2 - For LOW service cloud providers, the information system takes the following actions in the event of an audit processing failure: Overwrite oldest audit records.

SUPPLEMENTAL GUIDANCE

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; IRS1075; CJIS 5.6	AU-4, SI-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; and other relevant documents or records. Examine: Information system provides an automated alerting on error/failure capability. Test: Automated mechanisms implementing information system response to audit processing failures (i.e., halts processing or shuts down).	

AU-05(01): AUDIT STORAGE CAPACITY

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable system security plan), within a defined time period (defined in the applicable system security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system provides an automated alerting on disk capacity threshold reached capability. Test: Automated mechanisms implementing audit storage limit warnings.	

AU-05(02): REAL-TIME ALERTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system provides an alert in real-time to defined personnel, roles, and/or locations (defined in the applicable system security plan) when the following audit failure events occur: - Record log is full;	

- Auditing application reports an error; - Authentication logging failure; and - Encryption logging failure.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

REFERENCES	**RELATED CONTROLS**
CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; system security plan; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system provides an automated alerting on error/failure capability. Test: Automated mechanisms implementing real time audit alerts when organization-defined audit failure events occur.

AU-06: AUDIT REVIEW, ANALYSIS, AND REPORTING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS
The organization: a. Reviews and analyzes information system audit records in accordance with IS-Security Audit procedures for indication of inappropriate or unusual activity as defined within the Implementation Standards; and b. Reports findings to defined personnel or roles (defined in the applicable system security plan). **CMS-ARS:** a. Reviews and analyzes information system audit records no less often than weekly for indications of inappropriate or unusual activity as defined within the Implementation Standards; **IRS:** a. Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized FTI access b. Report findings according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0, Reporting Improper Inspections or Disclosures. **CJIS:** Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.
CONTROL IMPLEMENTATION STANDARDS
SPI: Std.1 - The applicant/bidder reviews system security logs on computing systems that access or store HHS Confidential Information for abnormal activity or security concerns on a regular basis. **CMS-ARS:** Low, Low Plus, Moderate, High:

Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.3 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.4 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.5 - Use automated utilities to review audit records no less often than every seventy-two (72) hours for unusual, unexpected, or suspicious behavior.

Low, Low Plus:
Std.6 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator accounts have not been created.
Std.7 - Inspect administrator groups on demand but no less often than once every thirty (30) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.

Moderate, High:
Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.

Moderate:
Std.7 - Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.

High:
Std.7 - Inspect administrator groups on demand but no less often than once every seven (7) days to ensure unauthorized administrator, system, and privileged application accounts have not been created.

CMS-MARS-E:
Std.1 - Review system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alert notification for technical personnel review and assessment.
Std.2 - Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies no less often than once within a twenty-four (24) hour period and on demand. Generate alerts for technical personnel review and assessment.
Std.3 - Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action.
Std.4 - Use automated utilities to review audit records no less often than weekly for unusual, unexpected, or suspicious behavior.
Std.5 - Inspect administrator groups on demand but no less often than once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.
Std.6 - Perform manual reviews of system audit records randomly on demand but no less often than once every thirty (30) days.
Std.7 - For service providers, the organization reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports finding to designated organizational officials.

IRS:
The Office of Safeguards recommends agencies identify events that may indicate a potential unauthorized access to FTI. This recommendation is not a requirement at this time, but agencies are encouraged to contact the Office of Safeguards with any questions regarding implementation strategies. Methods of detecting unauthorized access to FTI include matching audit trails to access attempts (successful or unsuccessful) across the following categories

Std.1 - Proactive Auditing Methods to Detect Unauthorized Access to FTI
a. Do Not Access List - Create a Do Not Access list to identify high-profile individuals or companies whose records have a high probability of being accessed without proper authorization
b. Time of Day Access - Identify suspicious behavior by tracking FTI accesses outside normal business hours

c. Name Searches - Detect potential unauthorized access by monitoring name searches (especially searches on the same last name as the employee)
d. Previous Accesses - Identify employee accesses to Tax Identification Numbers (TINs) that the employee has accessed in the past but currently does not have a case assignment or need to access
e. Volume - Monitor the volume of accesses a person performs and compare them to past case assignment levels
f. Zip Code - Determine whether an employee is accessing taxpayers whose address of record is geographically close to the employee's home or work location (i.e., same building, zip code, block)
g. Restricted TIN - Monitor all TINs associated with past employees' tax returns (e.g., self, spouse, children, businesses).

It is recommended the agency define a frequency in which the preceding categories are updated for an individual to ensure the information is kept current.

SUPPLEMENTAL GUIDANCE

Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority.

PII:
Periodic reviews and analysis of privacy logs are important for identifying indications of inappropriate or unusual activity that may signify a privacy incident or breach.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(g)(1)(D); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(C), 45 C.F.R. §164.312(b); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-7-16, M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	AC-2, AC-3, AC-6, AC-17, AR-4, AT-3, AU-7, AU-16, CA-7, CM-5, CM-8, CM-10, CM-11, IA-3, IA-5, IR-4, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; and other relevant documents or records.
Examine: Information system provides an anomalous behavior detection and reporting capability.
Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities.
Test: Use automated utilities in the review of audit records.
Test: Information system audit review, analysis, and reporting capability.

AU-06(01): PROCESS INTEGRATION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS: High & Moderate: Std.1 - Aggregated audit records from automated information security capabilities and service tools must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with HHS, CMS, State, and federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Audit records sources include systems, appliances, devices, services, and applications (including databases). (c) HHS Information Security directed audit information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by HHS and CMS, raw audit records must be available in an unaltered format to HHS Information Security. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to HHS Information Security.
SUPPLEMENTAL GUIDANCE
Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	AU-12, PM-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; and other relevant documents or records. Examine: Information system provides automated mechanisms to integrate audit review, analysis, and reporting processes to support investigation and response to suspicious activities. Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities. Test: Information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities.

AU-06(03): CORRELATE AUDIT REPOSITORIES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: High & Moderate: Std.1 - Correlated results from automated tools must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with HHS, CMS, State, and federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Repository sources include systems, appliances, devices, services, and applications (including databases); and (c) HHS Information Security directed repository information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by HHS and CMS, raw audit records must be available in an unaltered format to HHS Information Security. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to HHS Information Security.	
SUPPLEMENTAL GUIDANCE	
Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness.	

PII: Correlating and analyzing privacy audit logs across different log repositories and systems provides greater awareness of privacy incidents and breaches across the organization.	
REFERENCES	**RELATED CONTROLS**
Code: 5 U.S.C. §552a(g)(1)(D); FedRAMP Rev. 4 Baseline; OMB Memo: M-7-16; CJIS 5.6	AU-12, IR-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system audit records across different repositories; and other relevant documents or records. Examine: Information system provides the capability to analyze and correlate audit records generated across different repositories. Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities. Test: Automated mechanisms integrating audit review, analysis, and reporting processes.	

AU-06(05): INTEGRATION / SCANNING AND MONITORING CAPABILITIES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization integrates analysis of audit records with analysis of (one-or-more, defined in the applicable system security plan): vulnerability scanning information; performance data; information system monitoring information; and/or other defined data/information (defined in the applicable system security plan) collected from other sources, to further enhance the ability to identify inappropriate or unusual activity.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Aggregated vulnerability scanning information, performance data, and network monitoring information from automated tools must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Information sources include systems, appliances, devices, services, and applications (including databases); and (c) HHS Information Security directed information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw vulnerability scanning information, performance data, and network monitoring information must be available in an unaltered format to HHS Information Security. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to HHS Information Security.	
SUPPLEMENTAL GUIDANCE	
This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber-attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.	
REFERENCES	**RELATED CONTROLS**

Federal: NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	AU-12, IR-4, RA-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate audit records with analysis of vulnerability scanning information, performance data, and network monitoring information.
Test: Information system capability for centralizing review and analysis of audit records from multiple information system components.
Audit records with analysis of vulnerability scanning information, performance data, and network monitoring information must be analyzed for relevant security and privacy alerts. Additionally, collected information must be made available to HHS Information Security for aggregation and analysis at the CMS enterprise level.

AU-06(06): CORRELATION WITH PHYSICAL MONITORING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.
- Cross-organizational coordination leverages critical information from a variety of sources to more effectively respond to information security-related incidents that potentially affect organization operations, assets, and individuals.
- The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns.
- Effectiveness of event correlation depends on the quality of the data that goes into it. Organizations should establish logging standards and procedures to ensure that adequate information is collected and that the data is reviewed regularly.
- Consistent log timestamps facilitate effective event correlation.

REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-100, 800-61	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; system security plan; and other relevant documents or records.
Examine: Information system provides the capability to analyze and correlate required security data.
Test: Information system capability for centralizing review and analysis of audit records from multiple information system components.

AU-06(10): AUDIT LEVEL ADJUSTMENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
PII: The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
PII: Change of risk includes situations involving a potential breach of personally identifiable information (PII).	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-07-16	AR-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
PII: Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on: (i) law enforcement information; (ii) intelligence information; and/or (iii) other credible sources of information.	
ASSESSMENT METHODS AND OBJECTS	
PII: Examine: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; system security plan; other relevant documents or records. Examine: Information system provides the capability to adjust the level of audit review, analysis, and reporting. Interview: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting review, analysis, and reporting of audit information.	

AU-07: AUDIT REDUCTION AND REPORT GENERATION

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time marking of audit records.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. - Event collection and analysis software can perform event reduction by disregarding data that are not significant to information system security, potentially increasing its efficiency in network and storage resource needs. PII:	

To meet the deadlines associated with reporting loss of sensitive information, such as a breach of personally identifiable information (PII), it is necessary to have the ability to summarize audit information and generate customized audit reports.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.312(b) NIST SP: 800-137; OMB Memo: M-07-16, Att. 2; IRS-1075; CJIS 5.6	AU-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; and other relevant documents or records. Examine: Information system provides an audit reduction and report generation capability that meets defined requirements. Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities. Test: Audit reduction and report generation capability.	

AU-07(01): AUTOMATIC PROCESSING

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system provides the capability to process audit records for events of interest based on selectable event criteria.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. PII: To conduct efficient and effective remediation of loss of sensitive information, such as a breach of personally identifiable information (PII), it may be necessary to tailor the audit fields provided in audit reports. For example, it may be necessary to include the identities of individuals and the system resources involved to determine scope	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-07-16, Att. 2; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)	AU-2, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; information system audit records; and other relevant documents or records. Examine: Information system provides the capability to analyze and correlate required security data on defined criteria. Test: Audit reduction and report generation capability.	

AU-07(02): AUTOMATIC SORT AND SEARCH

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system provides the capability to sort and search audit records for events of interest based on the content of organization-defined audit fields within audit records.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
To conduct efficient and effective remediation of loss of sensitive information, such as a breach of personally identifiable information (PII), it may be necessary to tailor the organization of the audit report or to provide search functionality with audit reports that are generated. For example, if the PII breach involves only one or two users it may be most efficient to sort the audit report by user ID or to provide the ability to search on user ID within the audit report. Consideration must be given on admissibility as defined by the Federal Rules of Evidence.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-07-16, Att. 2; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b)	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) the organization defines audit fields within audit records in order to sort and search audit records for events of interest based on content of such audit fields; and (ii) the information system provides the capability to sort and search audit records for events of interest based on the content of organization-defined audit fields within audit records.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, analysis, and reporting tools; audit record criteria (fields) establishing events of interest; information system audit records; other relevant documents or records. Examine: Information system provides the capability to analyze and correlate required security data on defined criteria. Interview: Organizational personnel with audit reduction and report generation responsibilities; organizational personnel with information security responsibilities; system developers. Test: Audit reduction and report generation capability.	

AU-08: TIME STAMPS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, IRS, CJIS, CMS-ARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to UTC or GMT and is accurate to within one hundred (100) milliseconds. **IRS:** c. Compare and synchronize the internal information system clocks to an enterprise-wide authoritative time source. Where possible, synchronize enterprise time source to an external source (e.g., NIST, Naval Observatory).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Time stamps generated by the information system include date and time. Time is commonly expressed in UTC, a modern continuation of GMT, or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks	

synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. - The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns; and - Consistent log timestamps facilitate effective event correlation.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2, IRS1075; CJIS 5.6	AU-3, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; or other relevant documents or records. Examine: Information system provides required time stamping and synchronization. Interview: Organizational personnel with information system audit review, analysis, and reporting responsibilities. Test: Audit reduction and report generation capability.	

AU-08(01): SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Compares the internal information system clocks no less often than daily and at system boot with Organization defined NTP servers; and b. Synchronizes the internal clocks to the authoritative time source when the time difference is greater than one hundred (100) milliseconds. **CMS-ARS:** (a) one or more of the following federally maintained NTP stratum-1 servers: - NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi) - U.S. Naval Observatory Stratum-1 NTP Servers (http://tycho.usno.navy.mil/ntp.html); and - CMS designated internal NTP time servers providing an NTP Stratum-2 service to the above servers; and	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The information system synchronizes internal information system clocks at least hourly with: http://tf.nist.gov/tf-cgi/servers.cgi Std.2 - The organization selects primary and secondary time servers used by the National Institute of Standards and Technology (NIST) Internet time service. The secondary server is selected from a different geographic region than the primary server. Std.3 -The organization synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.	
SUPPLEMENTAL GUIDANCE	
This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. - The correlation of monitoring tools that usually work in isolation (e.g., host monitoring, network monitoring, anti-virus software) can provide an organization-wide view and in so doing, may reveal otherwise unseen attack patterns; and - Consistent log timestamps facilitate effective event correlation.	
REFERENCES	**RELATED CONTROLS**

Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-61, 800-100; CJIS 5.6	AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing time stamp generation; system security plan; information system design documentation; information system configuration settings and associated documentation; or other relevant documents or records. Examine: Information system provides required time stamping and synchronization. Test: Automated mechanisms implementing internal information system clock synchronization.	

AU-09: PROTECTION OF AUDIT INFORMATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
CONTROL IMPLEMENTATION STANDARDS	
High: Std.1 - Cryptographic mechanisms shall be employed to protect the integrity of audit information (e.g., log, and audit tools). **IRS:** The agency must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries. **CMS-ARS:** When audit information contains sensitive information, such as personally identifiable information (PII) or protected health information (PHI), it must be protected commensurate with the information's confidentiality impact level. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act. Protecting audit records from compromise by applying this control enhancement helps ensure their availability when needed.	
SUPPLEMENTAL GUIDANCE	
Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(i); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; OMB Memo: M-07-16; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.312(b); IRS1075; CJIS 5.6	AC-3, AC-6, AU-4(1), MP-2, MP-4, PE-2, PE-3, PE-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; and other relevant documents or records.	

Examine: Information system is configured to protect audit tools and data from unauthorized access. Test: Automated mechanisms implementing audit information protection. Examine tools, data files. Ensure file rotations retain required protections.

AU-09(02): AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system backs up audit records no less often than weekly onto a physically different system or system component than the system or component being audited.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The centralized audit servers must meet this control. Std.2 - The centralized audit server must be separated from the audit client information systems.	
SUPPLEMENTAL GUIDANCE	
This control is satisfied for servers forwarding audit records and information to a centralized audit server for aggregation and analysis.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-137; CJIS 5.6	AU-4, AU-5, AU-11
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing protection of audit information; system security plan; information system design documentation; information system configuration settings and associated documentation, system or media storing backups of information system audit records; information system audit records; and other relevant documents or records. Examine: The information system backs up audit records onto a physically different system or system component than the system or component being audited. Interview: Organizational personnel with auditing and accountability responsibilities.	

AU-09(03): CRYPTOGRAPHIC PROTECTION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. **CMS-ARS:** Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. PII: Using cryptographic mechanisms protects audit log integrity and the confidentiality of the information in the logs, including information related to privacy incidents and breaches. Audit information could be necessary to enforce criminal or civil penalties under the Privacy Act.	

In addition to cryptographic mechanisms to protect integrity, the confidentiality of personally identifiable information (PII) may require the use of encryption.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(i); OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.306(a)(1); 45 C.F.R. §164.312(a)(2)(iv)	AU-10, SC-12, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information system audit records; and other relevant documents or records. Examine: Information system implements FIPS 140-2-compliant cryptographic mechanisms to protect the integrity of audit information. Interview: Organizational personnel with auditing and accountability responsibilities.	

AU-09(04): ACCESS BY SUBSET OF PRIVILEGED USERS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable system security plan. **IRS:** The agency must authorize access to manage audit functionality only to designated security administrator(s) or staff other than the system and network administrator. System and network administrators must not have the ability to modify or delete audit log entries.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b)(1); FedRAMP Rev. 4 Baseline; CJIS 5.6	AC-5, AR-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; and other relevant documents or records. Interview: Organizational personnel with auditing and accountability responsibilities.	

AU-10: NON-REPUDIATION

Priority: P2	
Baseline(s): High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.	
CONTROL IMPLEMENTATION STANDARDS	

SUPPLEMENTAL GUIDANCE	
Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). PII: Non-repudiation is a critical element of accountability and accuracy of information in system history and logs, and it is important for investigating incidents and breaches.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(5) and (g)(1)(c); FISCAM: AC-2, AS-2; OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)	AR-4, AR-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system limits access to audit capabilities to authorized users and protects data from unauthorized modification. Test: Automated mechanisms implementing non-repudiation capability.	

AU-10(01): ASSOCIATION OF IDENTITIES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system: a. Binds the identity of the information producer with the information using an organization-defined strength of binding; and b. Provides the means for authorized individuals to determine the identity of the producer of the information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Digital signatures support accountability and non-repudiation by assuring data object originator authenticity (provides a reasonable level of certainty regarding who did what), data integrity (data has been manipulated by a verifiable person), and time-stamping for prevention of replay (time-stamping may also useful for gauging timeliness and relevance of personally identifiable information [PII]). Digital signatures bind the signer to the information the user signs. Digital signatures support accountability and non-repudiation by assuring data object originator authenticity (provides a reasonable level of certainty regarding who did what), data integrity (data has been manipulated by a verifiable person), and time stamping for prevention of replay (time-stamping may also useful for gauging timeliness and relevance of PII).	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(5) and (i)(3); OMB Memo: M-04-04; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.312(b); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(c)(2); 45 C.F.R. §164.312(e)(2)(i)	AC-4, AC-16
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if: (i) the organization defines the strength of binding to be employed between the identity of the information producer and the information; (ii) the information system binds the identity of the information producer with the information to the organization-defined strength of binding; and (iii) the information system provides the means for authorized individuals to determine the identity of the producer of the information.
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system Binds the identity of the information producer with the information as required. Interview: Organizational personnel with information system audit record retention responsibilities. Test: Automated mechanisms implementing non-repudiation capability.

AU-11: AUDIT RECORD RETENTION

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, high	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory (e.g., State and Federal Rules of Evidence) and HHS information retention requirements.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - When subject to a legal investigation audit records must be maintained until released by the investigating authority. Std.2 - Audit record retention must comply with applicable State of Texas, National Archives and Records Administration (NARA) or other authoritative mandate durations. **IRS:** Std.3 - The agency must retain audit records for the events identified in Section 9.3.3.2, Audit Events (AU-2) for seven (7) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements. **CMS-MARS-E:** Std.3 - Audit inspection reports, including a record of corrective actions, are retained by the organization for a minimum of three (3) years from the date the inspection was completed. Std.4 - The organization retains audit records online for at least ninety (90) days and further preserves audit records off-line for a period of ten (10) years. **CMS-ARS:** PII High & Moderate: PRIV.1 - Audit inspection reports, including a record of corrective actions, must be retained by the organization for a minimum of three (3) years from the date the inspection was completed.	
SUPPLEMENTAL GUIDANCE	
Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	AU-4, AU-5, AU-9, MP-6

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HHS: Policy for Monitoring Employee Use of HHS IT Resources; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit record retention; system security plan; organization-defined retention period for audit records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with information system audit record retention responsibilities.

AU-12: AUDIT GENERATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system:
a. Provides audit record generation capability for the following auditable events defined in AU-2a for all HHS information systems
b. Allows defined personnel or roles (defined in the applicable system security plan) to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the list of events defined in AU-2 with the content defined in AU-3.

CONTROL IMPLEMENTATION STANDARDS

CMS-MARS-E:
Std.1 - The information system provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed.

SUPPLEMENTAL GUIDANCE

Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records.

PII:
This control defines the technical aspects of how the privacy auditing requirements identified in controls AU-2 and AU-3 will be selected, generated and reviewed for compliance.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); IRS1075; CJIS 5.6	AC-3, AU-2, AU-3, AU-6, AU-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Audit and accountability policy; procedures addressing audit record generation; system security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.
Examine: Information system provides the required audit record generation capability.
Interview: Organizational personnel with information system audit record generation responsibilities.
Test: Automated mechanisms implementing audit record generation capability.

AU-12(01): SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL

Priority: P1

Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system compiles audit records from defined information system components (defined in the applicable system security plan) into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five (5) minutes.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Audit trails are time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.	
REFERENCES	**RELATED CONTROLS**
	AU-8, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records. Examine: Information system aggregates, correlates, and compiles audit records from client systems in a manner that supports defined time variance. Test: Automated mechanisms implementing audit record generation capability.	

AU-12(03): CHANGES BY AUTHORIZED INDIVIDUALS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system provides the capability for defined individuals or roles (defined in the applicable system security plan) to change the auditing to be performed on defined information system components (defined in the applicable system security plan) based on defined selectable event criteria (defined in the applicable system security plan) within minutes.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. PII: Changes to the audit of information systems containing sensitive information must be limited to a subset of authorized system administrators to ensure integrity of audit logs. This control requires organization to define the individuals or roles that would be able to make changes to audit generation requirements.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Circular A-130: 7.g. and 8.b(2)(c)(iii); 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R.§164.308(a)(2)	AU-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing audit record generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; and other relevant documents or records.	

Examine: Information system provides the capability for defined individuals or roles to change the auditing to be performed. Interview: Organizational personnel with information system audit record generation responsibilities.

AU-13: MONITORING FOR INFORMATION DISCLOSURE

Priority: P1	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The organization monitors open source information and/or information sites at an organization-defined frequency for evidence of unauthorized disclosure of organizational information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Open source information includes, for example, social networking sites.	
REFERENCES	**RELATED CONTROLS**
Federal: HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)	PE-03, SC-07
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing information disclosure monitoring; information system design documentation; information system configuration settings and associated documentation; monitoring records; information system audit records; other relevant documents or records. Interview: Organizational personnel with responsibilities for monitoring open source information and/or information sites; organizational personnel with information security responsibilities. Test: Automated mechanisms implementing monitoring for information disclosure.	

AU-16: CROSS-ORGANIZATIONAL AUDITING

Priority:	
Baseline(s):	Overlay(s): IRS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs organization-defined methods for coordinating organization-defined audit information among external organizations when audit information is transmitted across organizational boundaries.	
CONTROL IMPLEMENTATION STANDARDS	
IRS: This requirement applies to outsourced data centers or cloud providers. The provider must be held accountable to protect and share audit information with the agency through the contract. See Section 9.4.1, Cloud Computing Environments for additional cloud computing requirements, including language for cloud computing requirements. Also see Section 5.4, Controls over Processing for information pertaining to consolidated data centers.	
SUPPLEMENTAL GUIDANCE	
When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals.	
REFERENCES	**RELATED CONTROLS**
Federal: IRS1075	AU-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Audit and accountability policy; procedures addressing methods for coordinating audit information among external organizations; information system design documentation; information system configuration settings and associated documentation; methods for coordinating audit information among external organizations; information system audit records; other relevant documents or records. Interview: Organizational personnel with responsibilities for coordinating audit information among external organizations; organizational personnel with information security responsibilities. Test: Automated mechanisms implementing cross-organizational auditing (if applicable).

AU-16(02): SHARING OF AUDIT INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization provides cross-organizational audit information to any organization with whom audit information containing PII or PHI is shared based on MOUs, MOAs, or other data sharing agreements	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
As audit logs may contain PHI, when audit information is shared between organizations, an agreement addressing the handling, protection, and disclosure of PHI is required. Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations. MOUs, memoranda of agreement (MOAs), and other data sharing agreements must address protection of PHI, audit content confidentiality ensuring authorized disclosures, and assurance that sharing agreement define which audit events and results are both captured and shared.	
REFERENCES	**RELATED CONTROLS**
Federal: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(5)(ii)(C); 45 C.F.R. §164.312(b); 45 C.F.R. §164.314	CA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Audit and accountability policy; procedures addressing cross-organizational sharing of audit information; cross-organizational sharing agreements; data sharing agreements; other relevant documents or records. Interview: Organizational personnel with responsibilities for sharing cross-organizational audit information; organizational personnel with information security responsibilities.	

(CA) SECURITY ASSESSMENT AND AUTHORIZATION

The HHS organization requires that (i) an initial assessment of the security controls for key information systems is performed to determine if the controls are effective in their application; (ii) controls are monitored on an ongoing basis to ensure their continued effectiveness; (iii) information systems containing potential vulnerabilities due to deficiencies in their controls are documented and acknowledged by the HHS CISO and/or the CISO's designee and (iv) plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities are developed and implemented.

CA-01: SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls. b. Reviews and updates (as necessary) the current: 1. Security assessment and authorization policy at least every three (3) years; and 2. Security assessment and authorization procedures at least once every three hundred sixty five (365) days. **CMS-MARS-E:** b.1. Security assessment and authorization policy at least once every three hundred sixty five (365) days	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PII: The security assessment and authorization policy and procedures should address the strategy for including applicable privacy requirements and controls in the security program and information systems.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 164.308(a)(8); Homeland Security Presidential Directive (HSPD) 7: F(19); NIST SP: 800-12, 800-37, 800-100; OMB Memo: M-07-16, Att. 1; 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(ii); 45 C.F.R. §164.308(a)(2); IRS1075; CJIS 5.6	AR-1, AR-7, PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policies and procedures; other relevant documents or records. Interview: Organizational personnel with security assessment and authorization responsibilities.	

CA-02: SECURITY ASSESSMENTS

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops an information security and privacy control assessment plan that describes the scope of the assessment including:	

1. Security and privacy controls and control enhancements under assessment (including information security and privacy changes enacted by HHS and HHS CIO/CISO directives);
2. Assessment procedures to be used to determine control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities.
b. Assesses the security and privacy controls in the information system and its environment of operation as defined in implementation standards depending on the system categorization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
c. Produces a security assessment report (SAR) that documents the results of the assessment; and
d. Provides the results of the security and privacy control assessment within thirty (30) days after its completion, in writing, to the Information Security Officer, Information Owner(s)/Custodian(s) responsible for the system, and personnel responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

CMS-MARS-E:
b. The organization assesses the security and privacy controls in the information system and its environment of operation within every three hundred sixty-five (365) days in accordance with the current Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.
d. The organization provides the results of the security and privacy control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system.

IRS:
b. Assess the security controls in the information system and its environment at a minimum on an annual basis to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements
d. Provide the results of the security control assessment to the agency's Authorizing Official

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Information Security will perform a review of the state organization's information security program for compliance with DIR standards at least annually, based on business risk management decisions, by individual(s) independent of the information security program and designated by the state organization head or his or her designated representative(s).
Std.2 - At least once every two years, the state agency shall conduct an information security assessment of the agency's information resources systems, network systems, digital data, storage systems, digital data security measures, and information resources vulnerabilities. Not later than December 1 of the year in which the state agency conducts the assessment, the agency shall report the results of the assessment to the department of information resources (DIR), the governor, the lieutenant governor, and the speaker of the house of representatives.
Std.3 – Security assessments are in addition to the risk assessments conducted by Information Owners (see RA-3)

Low, Low Plus:
Std.4 – Systems may, at the direction of the HHS CISO, be required to undergo targeted or full security assessment. Unless required by the HHS CISO, the assessment team is not required to have a HHS CISO defined level of independence (See CA-02(01))

Moderate, High:
Std.4 – For newly implemented systems and systems undergoing a major change, a security assessment of affected controls must be conducted prior to issuing an authority to operate (ATO).
Std.5 – Systems must undergo a security assessment at least once every two (2) years.
Std.6 – Security assessments must be conducted by a team with HHS CISO defined level of independence (See CA-02(01))

Web & Mobile:
Std.7 - Conduct an evaluation to ensure that sensitive data is not being unnecessarily transported or stored.

CMS-MARS-E:

Std.8 - (MARS-E Std.1) An independent assessment of all security and privacy controls must be conducted before the Administering Entity's (AE) Authorizing Official issues the authority to operate for all newly implemented, or significantly changed, systems.
Std.9 - (MARS-E Std.2) CMS requires that an independent assessment of all security and privacy controls be conducted every three (3) years or with each major system change
Std.10 - (MARS-E Std.3) The annual security and privacy assessment requirement mandated by CMS requires all security and privacy controls attributable to a system to be assessed over a three (3) year period. To meet this requirement, a subset of the security and privacy controls shall be tested each year so that all controls are tested during a three (3)-year period. CMS provided guidance for conducting annual security and privacy assessments in the document, *Annual Security and Privacy Attestation Procedures for State-Based ACA Administering Entity Systems*.
Std.11 - (MARS-E Std.4) The business owner notifies CMS within thirty (30) days whenever updates are made to system security and privacy authorization artifacts or when significant role changes occur.

CJIS:
Std.8 - At a minimum, triennially audit all Criminal Justice Agencies (CJA) and Non-Criminal Justice Agencies (NCJA) which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
Std.9. - The FBI CJIS Division is authorized to conduct security audits of the CJIS System Agency (CSA)(e.g. HHS) and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

IRS:
Std.5 - Assess the security controls in the information system and its environment at a minimum on an annual basis

SUPPLEMENTAL GUIDANCE

Organizations assess security controls in organizational information system and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from NIST SP 800-53 Appendix F (main catalog) and NIST SP 800-53 Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by HHS, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The Federal Information Security Modernization Act (FISMA) requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives.

To satisfy annual assessment requirements, organizations can use assessment results from the following sources, including but not limited to: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness; and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical to protecting HHS operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the

above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control.

PII:
This control addresses the process of planning for and executing security assessments, the scope of which should include assessment of applicable privacy requirements.
Once the final security assessment is completed, update the associated Privacy Impact Assessment (PIA) to reflect the results of the security assessment.

REFERENCES	RELATED CONTROLS
State: TGC 2054.515 **State:** DIR Security Control Standards Catalog **Federal:** EIS-Policy 10.5.1; Code: 5 United States Code (U.S.C.) §552a(b); Executive Order: 13587; FedRAMP Rev. 4 Baseline; Federal Information Processing Standard (FIPS) Pub: 199; FISCAM: AS-1, SM-5; HIPAA: 45 C.F.R. §164.308(a)(8); HSPD 7: D(11), F(19); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-07-16 Att. 1, A.2.c, M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	AR-2, CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security assessment policy; procedures addressing security assessments; system security plan; security assessment plan; assessment evidence; and other relevant documents or records.
Examine: Information system is assessed in accordance with the assessment plan.

CA-02(01): INDEPENDENT ASSESSORS

Priority: P2

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs assessors or assessment teams with no operational responsibilities for the information system being assessed to conduct security control assessments.

CMS-MARS-E:
The organization employs assessors or assessment teams with CMS-defined level of independence to conduct security and privacy control assessments of the organization's information system.

CONTROL IMPLEMENTATION STANDARDS

CMS-MARS-E:
CMS provides guidance for employing independent assessors in the Framework of Independent Assessment (IA) of Security and Privacy Controls, located at:
https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

SUPPLEMENTAL GUIDANCE

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations.
Aos determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Aos also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to

make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments be conducted by individuals that are in the developmental, operational, or management chain of system owners; independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.	
REFERENCES	**RELATED CONTROLS**
FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing security assessments; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); and other relevant documents or records. Interview: Organizational personnel with security assessment responsibilities.	

CA-02(02): SPECIALIZED ASSESSMENTS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization includes as part of security control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing.	
CONTROL IMPLEMENTATION STANDARDS	
High & Moderate: Std.1 - Announced or unannounced in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing results must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) In-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing result information sources include traffic analysis tool systems, appliances, devices, services, and applications; and (c) HHS Information Security directed in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, raw results from in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, and performance/load testing must be available in an unaltered format to HHS Information Security. Std.3 - Raw security information/results from relevant automated tools must be available in an unaltered format to HHS Information Security.	
SUPPLEMENTAL GUIDANCE	
Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	PE-3, SI-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Security assessment and authorization policy; procedures addressing security assessments; system security plan; security assessment plan; security assessment report; assessment evidence; and other relevant documents or records. Interview: Organizational personnel with security assessment responsibilities.

CA-02(03): EXTERNAL ORGANIZATIONS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization accepts the results of an assessment of CMS information systems performed by CMS authorized independent assessors when the assessment meets CMS defined requirements and methodologies for performing assessments.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing security assessments; system security plan; security assessment plan; security assessment report; assessment evidence; and other relevant documents or records. Examine: Information detailing how assessment results are recorded and tracked. Example: - Is the organization actively using CFACTS to track results? - Is the organization remediating open findings being tracked? Interview: Organizational personnel with security assessment responsibilities.	

CA-03: SYSTEM INTERCONNECTIONS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements (ISA) or other comparable agreements (such as MOU/MOA, SLA, or specific contractual clause, so long as the appropriate interconnection detail is provided therein); b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; c. Reviews and updates the interconnection agreements on an ongoing basis, no less often than once every year and whenever significant changes (that can affect the security state of the information system) are implemented that could impact the validity of the agreement as a verification of enforcement of security requirements **CMS-ARS-E:** d. Only activates a system interconnection (including testing) when a signed interconnection agreement is in place.	

CMS-MARS-E:
d. The organization establishes system-to-system connections with CMS through the Fed2NonFed ISA process.

IRS:
d. Employ deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit FTI to connect to external information systems

CJIS:
d. Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI. See CJIS 5.6 Appendix D for examples of approved Information Exchange Agreements.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - If the interconnecting systems have the same Authorizing Official (AO) (or same primary operational IT infrastructure manager), an interconnection agreement document is not required; rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems.
Std.2 - Record each system interconnection in the SSP and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.
Std.3 - The interconnection agreement (or other applicable connection agreement) is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.
Std.4 - The HHS CIO, CISO, and Senior Official for Privacy (SOP) have the authority to order the immediate termination and/or suspension of any interconnection that, in the judgment of the CISO and the HHS Security Operations, presents an unacceptable level of risk to the HHS enterprise and/or mission.
Std.5 - The interconnection agreement must be fully signed and executed prior to any interconnection outside of the system boundary taking place for any purpose (within the constraints of the control [e.g., dedicated connections], including testing).

CJIS:
Std.1. - Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.
Std.2. - Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D of CJIS Security Policy for examples of Information Exchange Agreements.
Std.3. - There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.
Std.4. - Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit
2. Dissemination
3. Hit confirmation
4. Logging
5. Quality Assurance (QA)
6. Screening (Pre-Employment)
7. Security
8. Timeliness
9. Training
10. Use of the system
11. Validation

SUPPLEMENTAL GUIDANCE

This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations

carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. The HHS authorizing official determines the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same HHS Authorizing Official, an Interconnection Security Agreement (ISA) or other specific interconnection document (such as MOU/MOA, SLA, or specific contractual clause) is not required. Interface characteristics between the interconnecting information systems can be described in the security plans for their respective systems. Instead of developing an interconnection agreement (or other valid interconnection agreement forms such as MOU/MOA, SLA, etc.), organizations may choose to incorporate this information into formal contracts (so long as the appropriate detail is provided therein), especially if the interconnection is to be established between HHS and a nonfederal (private sector) organization. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require interconnection agreements and be subject to additional security controls.

PHI:
Consider the need for a MOU/MOA or Business Associate Agreement, and implement as necessary.

PII:
Interconnection agreements document whether and under what circumstances sensitive information, such as personally identifiable information (PII), can be shared between information systems in different authorization boundaries (e.g., an interface between systems owned by different agencies) over a dedicated or "always on" connection. Interconnection agreements communicate that sensitive information will be communicated via the connection and define the security parameters required to protect it. Interconnection agreements also provide a record of agreed upon terms and a document against which controls can be enforced and audited. Organizational policy dictates whether interconnection agreements are required for internal connections within an organization.

CJIS:
A Non-Criminal Justice Agency (NCJA) (government) designated to perform criminal justice functions for a Criminal Justice Agency (CJA) shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement.

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J of CJIS Security Policy for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system per authorization of Department of Justice (DOJ) Order 0904.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(o); FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-1, AS-2; HIPAA: 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.308(b)(3); 45 C.F.R. §164.504(e)(3); HSPD 7:F(19); NIST SP: 800-47; IRS1075; CJIS 5.6	AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; system security plan; information system design documentation; security assessment report; plan of action and milestones; MOUs and SLAs (as appropriate); and other relevant documents or records. Examine: Details about system interconnections. Interview: Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

CA-03(01): UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization prohibits the direct connection of a CJIS Information System to an external network, Internet, or information system without the use of controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels).	
CONTROL IMPLEMENTATION STANDARDS	
Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e., the device “fails closed” vs. “fails open”)	
SUPPLEMENTAL GUIDANCE	
Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified national security systems and external networks. This control enhancement is required for organizations processing, storing, or transmitting Controlled Unclassified Information (CUI).	
REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; information system configuration settings and associated documentation; security assessment report; information system audit records; other relevant documents or records. Interview: Organizational personnel with responsibility for managing direct connections to external networks; network administrators; organizational personnel with information security responsibilities; personnel managing directly connected external networks. Test: Automated mechanisms supporting the management of external network connections.

CA-03(02): CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization prohibits the direct connection of a classified, national security system to an external network without the use of use of controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels).	
CONTROL IMPLEMENTATION STANDARDS	
Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device “fails closed” vs. “fails open”)	
SUPPLEMENTAL GUIDANCE	
Organizations typically do not have control over external networks (e.g., the Internet). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between classified national security systems and external networks. In addition, approved boundary protection devices (typically managed interface/cross-domain systems) provide information flow enforcement from information systems to external networks.	
REFERENCES	**RELATED CONTROLS**

CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; security plan; information system design documentation; information system configuration settings and associated documentation; security assessment report; information system audit records; other relevant documents or records. Interview: Organizational personnel with responsibility for managing direct connections to external networks; network administrators; organizational personnel with information security responsibilities; personnel managing directly connected external networks. Test: Automated mechanisms supporting the management of external network connections.	

CA-03(03): UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization prohibits the direct connection of HHS information systems to an external network without the use of HHS-authorized boundary protection device.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Boundary protection devices protect systems containing sensitive information from unauthorized access by individuals outside the organization. A stateful inspection firewall is such a boundary protection device.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(10); OMB Memo: M-07-16; 45 C.F.R. §164.312(a)(1)	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Defines an unclassified, non-national security system whose direct connection to an external network is to be prohibited without the use of approved boundary protection device; (ii) Defines a boundary protection device to be used to establish the direct connection of an organization-defined unclassified, non-national security system to an external network; and (iii) Prohibits the direct connection of an organization-defined unclassified, non-national security system to an external network without the use of an organization-defined boundary protection device.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; system security plan; information system design documentation; security assessment report; plan of action and milestones; and other relevant documents or records. Examine: Information system implements functionality that provides an override of interconnections in manner that supports ease of use. Interview: Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.	

CA-03(05): RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The organization employs, and documents in the applicable system security plan, a deny-all, permit-by-exception, policy for allowing defined information systems (defined in the applicable security plan) to connect to external information systems.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as blacklisting (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as whitelisting (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. PII: External network connections open up the opportunity for intentional as well as inadvertent disclosure of sensitive information, such as personally identifiable information (PII). Email and file sharing applications are common points of vulnerability. Organizations require the ability to evaluate external network connections on a case-by-case basis to ensure such connections do not permit unauthorized access or disclosure of sensitive information.

REFERENCES	RELATED CONTROLS
Federal: Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; OMB Memo: M-07-16; 45 C.F.R. §164.312(a)(1); CJIS 5.6	CM-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Access control policy; procedures addressing information system connections; system and communications protection policy; information system interconnection security agreements; system security plan; information system design documentation; security assessment report; plan of action and milestones; and other relevant documents or records. Interview: Organizational personnel with responsibility for developing, implementing, or approving information system interconnection agreements.

CA-05: PLAN OF ACTION AND MILESTONES

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates and submits existing plan of action and milestones as corrective actions occur (not to exceed the POA&M expiration date) until the weakness/vulnerability is resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. **CMS-MARS-E**: b. The organization updates and submits the existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. c. The organization submits an updated POA&M to CMS every three (3) months. **IRS:** b. Update the existing POA&M on a quarterly basis, at a minimum, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities **CMS-ARS:** b. Updates and submits existing plan of action and milestones monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	

CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The POA&M should be developed and submitted in accordance with organizational procedures within thirty (30) days for high risk, sixty day (60) for moderate risk, and ninety days (90) for low risk finding of the date the finding becomes official. **CMS-MARS-E:** Std. 4. The Plan of Action and Milestones template is to be used for reporting POA&Ms to CMS and is found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ **IRS:** The POA&M must comprise of an all-inclusive tool or document for the agency to track vulnerabilities identified by the self-assessments, internal inspections, external audits and any other vulnerabilities identified for information systems that receive, process, store, or transmit FTI. Additional information is available in IRS 1075 Section 6.5, Plan of Action and Milestones.	
SUPPLEMENTAL GUIDANCE	
POA&Ms are key documents in security authorization packages and are subject to federal reporting requirements established by OMB.	
REFERENCES	**RELATED CONTROLS**
State: TAC 202.24(a)(5) **State:** DIR Security Control Standards Catalog **Federal:** EIS-Policy 10.5.3; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-6; HIPAA: 45 C.F.R. §164.308(a)(2), 164.308(a)(8); HSPD 7: F(19), G(24); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-02-01, M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	CA-2, CA-7, CM-4, PM-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; system security	

CA-05(01): AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing plan of action and milestones; information system design documentation, information system configuration settings and associated documentation; plan of action and milestones; and other relevant documents or records. Interview: Organizational personnel with plan of action and milestones (POA&M) development and implementation responsibilities. Test: Automated mechanisms for developing, implementing and maintaining POA&Ms.	

CA-06: SECURITY AUTHORIZATION

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The HHS organization:
a. Assigns a senior organizational official as the authorizing official for the HHS information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization in accordance with Implementation Standard 2.

CONTROL IMPLEMENTATION STANDARDS

Low, Low Plus, Moderate, High:
Std.1 - The Information Owner must notify HHS Information Security of significant changes to architecture, security posture, or other items that could cause degradation or unexpected results in security monitoring, detection, response, and mitigation activities prior to making a change.
Std.2 - The security authorization is updated:
- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and

Std.3 - Approval of security risk acceptance, transference, or mitigation decisions shall be the responsibility of:
a. The information security officer or his or her designee(s), in coordination with the information owner, for systems identified with a low or moderate residual risk.
b. The state agency head (or designees) for all systems identified with a residual High Risk.
Std.4 - Any exceptions shall be justified, documented, and communicated as part of the risk assessment process.

CMS-ARS, IRS, CJIS, CMS-MARS-E, VA:
Std.2 - The security authorization is updated:
- Within every three (3) years;
- When significant changes are made to the system;
- When changes in requirements result in the need to process data of a higher sensitivity;
- When changes occur to authorizing legislation or federal requirements that impact the system;
- After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and
- Prior to expiration of a previous security authorization.

SUPPLEMENTAL GUIDANCE

Security authorizations are official management decisions, conveyed through authorization decision documents, by the HHS CIO or his/her designated representative (i.e., authorizing officials) to authorize operation of information systems and to explicitly accept the risk to HHS operations and assets, individuals, other organizations, and the Nation based on the implementation of agreed-upon security controls. Explicit authorization to operate the information system is provided by the HHS CIO or his/her designated representative prior to a system being placed into operations. Through the security authorization process, the HHS CIO is accountable for security risks associated with the operation and use of HHS information system.
OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. Continuous monitoring programs can satisfy three-year reauthorization requirements, so separate reauthorization processes are not necessary. Through the employment of comprehensive continuous monitoring processes, critical information contained in authorization packages (i.e., security plans, security assessment reports, and plans of action and milestones) is updated on an ongoing basis, providing the HHS CIO and information system owners with an up-to-date status of the security state of organizational information systems and environments of operation. To reduce the administrative cost of security reauthorization, the HHS CIO uses results of the continuous monitoring processes to the maximum extent possible as the basis for rendering a reauthorization decisions.

PHI:
The senior-level executive should be one of the following: HIPAA Security Officer, Authorizing Official, Program Manager, Information System Security Manager (ISSM), or Information System Security Officer (ISSO).

PII: One of the considerations for the "go/no go" decision when authorizing (or re-authorizing) an information system is whether applicable privacy requirements have been met.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC 202.20(6); 202.25(4); TAC 202.21(c); DIR Security Control Standards Catalog **Federal:** Code: Pub. L. No. 107-347, §208; 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-2; HIPAA: 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii); HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04; OMB Circular A-130; IRS1075; CJIS 5.6	CA-1, CA-2, CA-7, PM-9, PM-10
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); and other relevant documents or records. Interview: Organizational personnel with security authorization responsibilities	

CA-07: CONTINUOUS MONITORING

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The HHS organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of defined metrics to be monitored; b. Establishment of defined frequencies for monitoring and defined frequencies for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the HHS organizational continuous monitoring strategy; d. Ongoing security status monitoring of HHS organization-defined metrics in accordance with the HHS organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of HHS organization and the HHS information systems to applicable personnel monthly. **CMS-ARS:** a. Establishment of defined metrics (defined in the applicable system security plan) to be monitored based on the organization security goals and objectives and in accordance with the basic requirements set forth in NIST SP 800-137; b. Establishment of defined frequencies (defined in the applicable system security plan), but no less than once every 72 hours, for monitoring and defined frequencies (defined in the applicable system security plan), but no less than once every 72 hours, for assessments supporting such monitoring; **CMS-MARS-E, IRS:** a. Establishment of organizationally defined metrics (defined in the applicable security plan) to be monitored annually, at a minimum **CMS-MARS-E:** h. Reporting the security status of AE systems to defined personnel or roles (defined in the applicable security plan) at organizational-defined frequency, and reporting to CMS as specified in the Implementation Standard	

CONTROL IMPLEMENTATION STANDARDS
Std.1 - When subject to a legal investigation (e.g., Insider Threat), continuous monitoring records must be maintained until released by the investigating authority. Std.2 - Monitors systems, appliances, devices, and applications (including databases). Std.3 - HHS Information Security provides oversight of information security and privacy, to include SIEM, for each System operating by or on behalf of HHS. **CMS-ARS:** PHI: Consider using automated tools and mechanisms for system activity review. The effectiveness of continuous monitoring of various activities, for example, failed or successful log-ins, inappropriate file access, detecting and reporting on malicious code/viruses through network transmission, is enhanced through the use of approved automated tools. PII: The state of security controls can directly correlate to privacy risk. Continuous monitoring supports the identification of issues that could result in unauthorized access to sensitive information such as PII, data quality issues, and other concerns, including privacy, that are supported by security controls.
SUPPLEMENTAL GUIDANCE
Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-5; HHS: Policy for Monitoring Employee Use of HHS IT Resources; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(5)(ii)(C) HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-11-33, M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	AR-4, CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; procedures addressing configuration management; system security plan; security assessment report; plan of action and milestones; information system monitoring records; configuration management records, security impact analyses; status reports; and other relevant documents or records. Examine: Information system is integrated into organizational and HHS continuous monitoring program. Interview: Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities.

CA-07(01): INDEPENDENT ASSESSMENT

Priority: P2

Baseline(s): Moderate, high	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs assessors or assessment teams with HHS CISO defined level of independence to monitor the security controls in the information system on an ongoing basis.

CMS-MARS-E:
The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs assessors or assessment teams with CMS-defined level of independence to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy security control assessment requirements.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

CMS-ARS:
An independent assessor (defined in the Risk Management Handbook (RMH), Volume 1, Chapter 10, "CMS Risk Management Terms, Definitions, and Acronyms") may be any internal/external agent or team that is capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management chain-of-command associated with the information system or to the determination of control effectiveness. Since these determinations are somewhat subjective, the HHS CISO retains the ultimate authority to make final judgments on the independence of any assessor. In addition see CMS IS2P2 section entitled Risk Management Framework RMF (CMS-RMF-1.8).

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: F(19); NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	AC-9, CA-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.
Interview: Organizational personnel with continuous monitoring responsibilities

CA-08: PENETRATION TESTING

Priority: P2

Baseline(s): Moderate, High	Overlay(s): Web & Mobile, HIPAA, DIR, CMS-ARS

CONTROL REQUIREMENTS

The organization conducts penetration testing on Internet facing websites and mobile applications that access, create, disclose, receive, transmit, maintain, or store HHS confidential data prior to the Information System being granted an Authority to Operate.

CMS-ARS:
The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components or whenever there has been a significant change to the system. As a minimum, penetration testing must be conducted to determine:
a. How well the system tolerates real world-style attack patterns;
b. The likely level of sophistication an attacker needs to successfully compromise the system;

c. Additional countermeasures that could mitigate threats against the system; and
d. Defenders' ability to detect attacks and respond appropriately.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - Conduct internal and external penetration testing as needed but no less often than once every three hundred sixty-five (365) days in accordance with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements.
Std.2 - Penetration tests are performed when new risks and threats potentially affecting the system/applications are identified and reported or upon request from CMS.
Std.3 - Penetration test scanning includes evaluation of embedded structures (e.g., content that can be changed without reloading the anchor content) and interactive content.
Std.4 - Penetration test scanning results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Penetration test information sources include systems, appliances, devices, services, and applications (including databases).
(c) HHS Information Security directed penetration test information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.5 - Penetration testing on a production system must be conducted in a manner that minimizes risk of information corruption or service outage.
Std.6 - Raw security information/results from relevant automated tools must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of internal and external adversaries in carrying out hostile cyber-attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.

PII:
When user session information and other PII is captured or recorded during penetration testing, ensure relevant privacy controls are addressed.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; NIST SP: 800-115; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g. and 8.b(3)	AP-1, AP-2, SA-12, TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; and other relevant documents or records..
Interview: Organizational personnel with penetration testing responsibilities.

Penetration test results must be made available to HHS Information Security for review, aggregation, and analysis at the enterprise level.

CA-08(01): INDEPENDENT PENETRATION AGENT OR TEAM

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.	
CONTROL IMPLEMENTATION STANDARDS	
High & Moderate: Std.1 - The independent penetration agent or penetration team must be a HHS CISO approved independent penetration test vendor.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-115; OMB Memo: M-14-03, M-15-01, M-16-04	CA-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; and other relevant documents or records. Interview: Organizational personnel with penetration testing responsibilities. Independent penetration test team must be a CMS Information Security and Privacy Group (ISPG) -approved source.	

CA-09: INTERNAL SYSTEM CONNECTIONS

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Authorizes connections of defined internal information system components or classes of components (defined in the applicable system security plan) to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate and High: Std.1 - The security plan will identify the types of personally owned equipment that may be internally connected with organizational information systems and networks: - Compliant with HHS policies on use of personally owned equipment	
SUPPLEMENTAL GUIDANCE	
This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example PII: Include privacy requirements in the Information Connection Document (or equivalent such as an Interconnection Security Agreement or an Authority to Connect package), specifically addressing the collection authority, compatibility of purpose for use, and need for recipient of information to achieve specific business purpose.	

Documentation must also address responsibilities of the receiving information system for protecting personally identifiable information (PII).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g. and 8.b(3)(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1); CJIS 5.6	AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4, UL-01, UL-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; and other relevant documents or records. Interview: Organizational personnel with component connection authorization responsibilities.	

CA-09(01): SECURITY COMPLIANCE CHECKS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system performs security compliance checks, as defined by HHS Policy, on constituent system components prior to the establishment of the internal connection.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Security compliance checks may include an assessment, prior to initial connection, of specific components, e.g., printers, based on sensitivity of personally identifiable information (PII) processed by that component. Any change to the components' security posture would require a re-verification of the configuration settings.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130: 7.g. and 8.b(3)(b); 45 C.F.R. §164.312(a)(1); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.306(a); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1)	CM-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
PII: Determine if the information system performs security compliance checks on constituent system components prior to the establishment of the internal connection.	
ASSESSMENT METHODS AND OBJECTS	
PII: Examine: Security assessment and authorization policy; procedures addressing continuous monitoring of information system security controls; system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. Interview: Organizational personnel with component connection authorization responsibilities.	

(CM) CONFIGURATION MANAGEMENT

The HHS organization (i) establishes and maintains baseline configurations and inventories of HHS information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establishes and enforces

security configuration settings for information technology products employed in HHS information systems.

CM-01: CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates (as necessary) the current: 1. Configuration management policy within every three (3) years; and 2. Configuration management procedures at least once every three hundred sixty five (365) days. **CMS-MARS-E:** b.1. Configuration management policy at least once every three hundred sixty five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The configuration management process and procedure is documented to define configuration items at the system and component level (e.g., hardware, software, workstation); monitor configurations; and track and approve changes prior to implementation, including, but not limited to, flaw remediation, security patches, and emergency changes (e.g., unscheduled changes such as mitigating newly discovered security vulnerabilities, system crashes, replacement of critical hardware components). Std.2 - The Chief Information Security Officer (CISO) is responsible for development and recommending procedures and practices, in cooperation with the agency Information Resources Manager; information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** EIS-Policy 10.6; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-1, SM-1, SM-3; NIST SP: 800-12, 800-100; IRS1075; CJIS 5.6	PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy and procedures; other relevant documents or records. Interview: Organizational personnel with configuration management and control responsibilities.	

CM-02: BASELINE CONFIGURATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
CONTROL IMPLEMENTATION STANDARDS
CMS-ARS: Low, Low Plus, Moderate, High Std.1 - Baselines will be distilled from government, industry, and vendor standards and best practices. Std.2 - Deployed configuration baselines include security updates. Std.3 - Configuration baseline requirements apply to all systems, devices, appliances, and applications.
SUPPLEMENTAL GUIDANCE
This control establishes baseline configurations for information systems and system components, including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. **IRS:** The Office of Safeguards recommends using SCSEMs provided on the Office of Safeguards website for developing an information system baseline configuration.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-128; IRS1075; CJIS 5.6	CM-3, CM-6, CM-8, CM-9, PM-5, PM-7, SA-10

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records. Examine: Information system is configured to defined baseline and baseline is updated to document current configuration. Examine: Baselines include implementation of government, industry, and vendor standards and best practices.

CM-02(01): REVIEWS AND UPDATES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The HHS organization reviews and updates the baseline configuration of HHS information systems: a. At least every two years or; b. When required due to upgrades, patches, or major system changes/upgrades and; c. As an integral part of HHS information system component installations and upgrades. **CMS-ARS:** a. At least every one hundred eight (180) days for High systems or three hundred sixty-five (365) days for Moderate systems; **CMS-MARS-E, IRS:**	

a. At least every three hundred sixty-five (365) days.

CMS-ARS, CMS-MARS-E:
b. When configuration settings change due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, and replacement of critical hardware components), and major system changes/upgrades.
c. As an integral part of information system component installations, upgrades, and updates to applicable governing standards (implemented within the 365 days specified in number 1 above).
d. Supporting baseline configuration documentation must reflect the ongoing implementation of operational configuration baseline updates, either directly or by policy.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Moderate & High:
Std.1 - Supporting baseline configuration documentation must reflect ongoing implementation of operational configuration baseline updates, either directly or by policy.

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-128; CJIS 5.6	CM-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; and other relevant documents or records.
Interview: Organizational personnel with configuration change control responsibilities.

CM-02(02): AUTOMATION SUPPORT FOR ACCURACY / CURRENCY

Priority: P1

Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8(2) for organizations that choose to combine information system component inventory and baseline configuration activities.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; Office of Management and Budget (OMB): M-14-03, M-15-01; NIST SP: 800-37, 800-100, 800-128	CM-7, RA-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records.
Test: Automated mechanisms implementing baseline configuration maintenance.

CM-02(03): RETENTION OF PREVIOUS CONFIGURATIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization retains older versions of baseline configurations of the information system as deemed necessary to support rollback.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate, High: Std.1 - No less than one (1) older baseline must be maintained.	
SUPPLEMENTAL GUIDANCE	
Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.	
REFERENCES	**RELATED CONTROLS**
FedRAMP Rev. 4 Baseline; NIST SP: 800-34, 800-100, 800-128; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; historical copies of baseline configurations; and other relevant documents or records.	

CM-02(06): DEVELOPMENT AND TEST ENVIRONMENTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration.	
CONTROL IMPLEMENTATION STANDARDS	
High: Std.1 - The organization must provide separated environments where execution and analysis of data may present an enhanced risk to the system.	
SUPPLEMENTAL GUIDANCE	
Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-128	CM-4, SC-3, SC-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; and other relevant documents or records. Test: Automated mechanisms implementing baseline configuration environments.	

CM-02(07): CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, VA
CONTROL REQUIREMENTS	
The organization: a. Issues dedicated information systems, system components, or devices with stringent configurations (e.g., FIPS 140-2 for encryption) to individuals traveling to locations that the organization deems to be of significant risk; and b. Applies security safeguards to the devices (i.e., detailed inspection of the device for physical tampering, purging or reimaging the hard disk drive/removable media) when the individuals return.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-128	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; and other relevant documents or records. Interview: Organizational personnel with configuration change control responsibilities.	

CM-03: CONFIGURATION CHANGE CONTROL

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for a minimum of three (3) years after the change; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through the HHS change control board that convenes frequently enough to accommodate change requests. **CMS-ARS, CMS-MARS-E:** g. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or HHS change control board that convenes frequently enough	

to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.

CONTROL IMPLEMENTATION STANDARDS

Std-1. Any change affecting the incident response (IR) computing environment (HVAC, water, plumbing, alarms, etc.) must be coordinated with the appropriate IT staff to ensure compliance with the change management process.

CMS-MARS-E:
Std.2 - The system owner coordinates and provides oversight for configuration change control activities through organization-defined configuration change control element (e.g., committee or board) that convenes according to organization-defined frequency and according to organization-defined configuration change conditions.
Std.3 - The system owner defines the configuration change control element and the frequency or conditions under which it is convened.
Std.4 - The organization establishes a central means of communicating significant changes to or developments in the information system or environment of operations that may affect its business agreements/contracts with CMS and business partners, and services to the business owner and associated service consumers (e.g., electronic bulletin board, or web status page). The means of communication are approved and accepted by the system owner. The means of communication with CMS about significant changes must follow the Change Reporting Procedures for State-Based Administering Entity Systems established by CMS, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
Std.5 - In establishing contracts with non-Exchange entities, the organization requires the non-Exchange entity to inform the organization of any changes in its administrative, technical, or operational environment defined as material within the contract.

SUPPLEMENTAL GUIDANCE

Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3, CM-6; NIST SP: 800-128; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(2)(ii); IRS1075; CJIS 5.6	CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records.
Examine: Organization facilitates required oversight of privacy reporting by CMS (including coordination and cooperation with the CMS Cybersecurity Infrastructure Center [HHS Information Security]).
Interview: Organizational personnel with configuration change control responsibilities.

CM-03(01): AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to:
a. Document proposed changes to the information system;
b. Notify designated approval authorities (defined in the SSP) of proposed changes to the information system;
c. Request change approval per the system configuration management documentation;
d. Highlight proposed changes that have been waiting an approval decision, or have not been approved, for longer than change management procedure (defined in the SSP) requires;
e. Prohibit changes to the information system until approvals are received;
f. Document all changes to the information system; and
g. Notify stakeholders when approved changes are completed.
A list of potential stakeholders must include, but is not limited to the following:
a. Change Control Board (CCB);
b. Configuration Management Executive;
c. Chief Risk Officer (CRO);
d. Cyber Risk Advisor (CRA);
e. ISSO;
f. Program Manager;
g. Data Guardian;
h. Information System Owner (ISO); and
i. Information System Administrator.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; and other relevant documents or records.
Test: Automated mechanisms implementing configuration change control.

CM-03(02): TEST / VALIDATE / DOCUMENT CHANGES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If

testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems). - To better secure IT infrastructure, configuration management procedure should include use of a security configuration checklist (sometimes called a lockdown, hardening guide, or benchmark) to help configure systems to a particular operating environment. - Security authorization (authorization to operate given identified risk and security controls) is maintained when proposed or actual changes to the information system, and their suspected impact on the security of the system, are documented and continuously monitored for compliance. - Configuration Management process includes the following steps: 1. Identify change; 2. Evaluate change request; 3. Approve, Deny or Defer implementation of the change; 4. Implement the approved change; and 5. Continuously monitor change for acceptable operation.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-100; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records. Interview: Organizational personnel with configuration change control responsibilities.	

CM-03(04): SECURITY REPRESENTATIVE

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization requires an information security representative to be a member of the Change Control Board.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3.	
REFERENCES	**RELATED CONTROLS**
CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; procedures addressing information system configuration change control; configuration management plan; security plan; other relevant documents or records. Interview: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for configuration change control.	

CM-03(06): CRYPTOGRAPHY MANAGEMENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
PII: The organization ensures that all cryptographic mechanisms used to provide protection to sensitive information are under configuration management.	
CONTROL IMPLEMENTATION STANDARDS	
PII: When encrypting personally identifiable information (PII), management processes must be in place to ensure future access to such data.	
SUPPLEMENTAL GUIDANCE	
PHI: When encrypting PHI, there must be management processes in place to ensure future access to such data.	
REFERENCES	**RELATED CONTROLS**
	SC-8, SC-12, SC-13, SC-28
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
PII: Determine if the organization: (i) defines security safeguards provided by cryptographic mechanisms that are to be under configuration management; and (ii) ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.	
ASSESSMENT METHODS AND OBJECTS	
PII: Examine: Configuration management policy; configuration management plan; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records. Interview: Organizational personnel with configuration change control responsibilities.	

CM-04: SECURITY IMPACT ANALYSIS

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization analyzes changes to the information system to determine potential security and privacy impacts prior to change implementation. **CMS-ARS, CMS-MARS-E:** Activities associated with configuration changes to the information system are audited.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - All security-related information resources changes shall be approved by the information owner through a change control process. Std.2 - Approval shall occur prior to implementation by the state organization or independent contractors. **CMS-MARS-E:** Std.3 - A security Impact Analysis report is required as part of change reporting to CMS. The Change Reporting Procedures for State-Based Administering Entity Systems established by CMS can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers [ISSO], Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation	

and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. PII: When analyzing changes to the information system, the impacts to privacy are also considered. If necessary, conduct a privacy impact assessment.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** E-Government Act of 2002 (Pub. L. No. 107-347), §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; NIST SP: 800-128; OMB Memo: M-03-22; 45 C.F.R. §164.308(a)(1)(ii)(A); 45 C.F.R. §164.308(a)(1)(ii)(B); 45 C.F.R. §164.308(a)(8); IRS1075; CJIS 5.6	AR-2, CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing security and privacy impact analysis for changes to the information system; security and privacy impact analysis documentation; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records. Interview: Organizational personnel with responsibilities for determining security and privacy impacts prior to implementation of information system changes.	

CM-04(01): SEPARATE TEST ENVIRONMENTS

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate, High: Std.1 - Test environments shall be kept either physically or logically separate from production environments. Copies of production data shall not be used for testing unless the data has been authorized for public release. Std.2 - Confidential production data will not be used for testing purposes unless it has been de-classified/de-identified or a valid risk exception has been approved in accordance with IS-Controls section 2.4.3, *Risk Acceptance*. If an exception is approved to use confidential data for testing that cannot be de-classified/de-identified, the test environment must meet the same security control requirements as the production system and the confidential data must be removed from the non-production environment immediately upon completion of the required testing. **CMS-ARS-E/CMS-MARS-E:** Std.2 - Processing or storing of Personally Identifiable Information (PII) in test environments is prohibited.	
SUPPLEMENTAL GUIDANCE	
Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). PII:	

If personally identifiable information (PII) is used in the test environment, then the same controls required for systems containing PII must be applied to the test environment. Simulated PII information should be used to the maximum extent practicable when testing system functionality.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(10); OMB Circular A-130: 7.g.; CJIS 5.6	AP-2, AR-3, DM-2, DM-3, SA-11, SA-15(9), SC-3, SC-7, UL-01
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; information system test and operational environments; and other relevant documents or records. Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.	

CM-04(02): VERIFICATION OF SECURITY FUNCTIONS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E, CJIS
CONTROL REQUIREMENTS	
The organization must ensure changes in information system security functions are verified: a. To be implemented per approved design; b. To integrate and operate as intended; and c. To produce expected results.	
CONTROL IMPLEMENTATION STANDARDS	
High & Moderate: Std.1 - Any system, including development and test, that contains and/or processes sensitive information (e.g., personally identifiable information [PII]) must verify security functions as per this control. Std.2 - The system's security functions must be continuously monitored and evaluated to ensure they are operating as intended and changes do not have an adverse effect on system performance. Std.3 - Actions must be taken to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements, and is an approved system configuration.	
SUPPLEMENTAL GUIDANCE	
Implementation in this context refers to installing changed code in the operational information system. In general, the goal is to verify that system changes do not adversely impact security functions and the system's ability to meet mission requirements. PII: If a system change is made, verification of Privacy Overlay security control functions is required to ensure continued compliance with privacy-related statutes and regulations.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(10); OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(7)(ii)(D); 45 C.F.R. §164.308(a)(8); 45 C.F.R. §164.316(b)(2)(iii); CJIS 5.6	SA-11
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the information system; security impact analysis documentation; change control records; information system audit records; and other relevant documents or records. Interview: Organizational personnel with responsibilities for determining security impacts prior to implementation of information system changes.	

CM-05: ACCESS RESTRICTIONS FOR CHANGE

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CMS-ARS, CMS-MARS-E:
Records reflecting all such changes must be generated, reviewed, and retained.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; NIST SP: 800-100; IRS1075; CJIS 5.6	AC-3, AC-6, PE-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities.
Test: Change control process and associated restrictions for changes to the information system.

CM-05(01): AUTOMATED ACCESS ENFORCEMENT / AUDITING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The information system enforces access restrictions and supports auditing of the enforcement actions.

CMS-MARS-E:
The organization employs automated mechanisms to enforce access restrictions to configuration change information and support auditing of the enforcement actions

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Cloud Moderate:
CSP.1 - For cloud service providers, this Standard replaces the above Enhancement. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-100; CJIS 5.6	AU-2, AU-6, AU-12, CM-3, CM-6

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; and other relevant documents or records.
Test: Mechanisms implementing access restrictions for changes to the information system.

CM-05(02): REVIEW SYSTEM CHANGES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS

The organization reviews information system changes:
a. At least once a week; and
b. When unauthorized changes or unexpected levels of system performance are indicated.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The system configuration must be continuously monitored as a supplemental information source for the review processes.
Std.2 - Information system changes must be verified to meet system mission and user requirements.

SUPPLEMENTAL GUIDANCE

Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. The results of the review includes evidence of control effectiveness and recommendations for correcting any deficiencies are documented.

REFERENCES	RELATED CONTROLS
Federal: NIST SP: 800-37, 800-100; CJIS 5.6	AU-6, AU-7, CM-3, CM-5, PE-6, PE-8

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records

CM-05(03): SIGNED COMPONENTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The information system prevents the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers,

and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication.	
REFERENCES	**RELATED CONTROLS**
FedRAMP Rev. 4 Baseline	CM-7, SC-13, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records. Test: Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate. Self-signed certificates are disallowed.	

CM-05(05): LIMIT PRODUCTION / OPERATIONAL PRIVILEGES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization: a. Limits privileges to change information system components and system-related information within a production or operational environment; and b. Reviews and reevaluates the privileges available to users authorized for privileged access no less frequently than once every three months.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AC-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the information system; list of critical software programs to be prohibited from installation without an approved certificate; information system design documentation; information system architecture and configuration documentation; system security plan; change control records; information system audit records; and other relevant documents or records. Test: Information system mechanisms preventing installation of software programs not signed with an organization-approved certificate. Self-signed certificates are disallowed.	

CM-05(06): LIMIT LIBRARY PRIVILEGES

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization limits privileges to change software resident within software libraries.	
CONTROL IMPLEMENTATION STANDARDS	

SUPPLEMENTAL GUIDANCE	
Software libraries include privileged programs.	
REFERENCES	**RELATED CONTROLS**
CJIS 5.6	AC-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; configuration management plan; information system design documentation; information system architecture and configuration documentation; information system configuration settings and associated documentation; change control records; information system audit records; other relevant documents or records.
Interview: Organizational personnel with information security responsibilities; system/network administrators.
Test: Organizational processes for managing access restrictions to change; automated mechanisms supporting and/or implementing access restrictions for change.

CM-06: CONFIGURATION SETTINGS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using the latest security configuration baselines established by HHS, The Center for Internet Security (CIS), U.S. Government Configuration Baselines (USGCB), or the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

IRS:
The agency must:
a. Establish and document configuration settings for IT products that receive, process, store, or transmit FTI using Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools) that reflect the most restrictive mode consistent with operational requirements

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Use of HHS approved Operating System (OS)
(a) HHS-specific minimum security configurations must be used for the following OS and Applications:
1. HHS approved CIS Windows Standards (e.g., Microsoft supported versions only); and
(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the HHS hierarchy for implementing security configuration guidelines is:
1. NIST NCP
2. The Center for Internet Security [CIS]
3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
4. National Security Agency (NSA) STIGs;
5. In situations where no guidance exists, coordinate with HHS Information Security for guidance.
6. All deviations from existing NCP, CIS, DISA and/or NSA configurations must be documented.

SPI:
Std.2 - The applicant/bidder implements computer security configurations or settings for all computers and systems that access or store HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)

CMS-MARS-E:
Std.1 - Security configuration guidelines may be developed by different federal agencies. Therefore, it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows:
1. National Institute of Standards and Technology (NIST)
2. CMS
3. Defense Information Systems Agency (DISA)
4. Office of Management and Budget (OMB)
5. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group, such as The Center for Internet Security (CIS) checklists.
6. The organization ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available)

IRS:
Std.1 - The authoritative source for platform checklists used by the Office of Safeguards is the NIST Checklist Program Repository (http://checklists.nist.gov). Office of Safeguards SCSEMs may include compliance requirements from one or more of the following security benchmarks:
1. United States Government Configuration Baseline (USGCB)
2. Center for Internet Security (CIS) Benchmarks
3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS)
4. National Security Agency (NSA) Configuration Guides

CMS-ARS:
Std.1 - Use of HHS approved Operating System (OS)
(a) HHS-specific minimum security configurations must be used for the following OS and Applications:
1. HHS approved CIS Windows Standards (e.g., Microsoft supported versions only); and
(b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the HHS hierarchy for implementing security configuration guidelines is:
1.The Center for Internet Security [CIS]
2. USGCB;
3. NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order;
4. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG);
5. National Security Agency (NSA) STIGs;
6. In situations where no guidance exists, coordinate with HHS Information Security for guidance.
7. All deviations from existing CIS, USGCB, NCP, DISA and/or NSA configurations must be documented.

SUPPLEMENTAL GUIDANCE

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline.
Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the USGCB which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems.

Legacy operating systems without ongoing vendor support, such as Windows XP or older desktop OS, Windows Server 2003 or older server OS, Solaris 9 or older OS, or Red Hat Linux 9 or older, are only permissible if documented within the Risk Assessment and System Security Plan and authorized by the Authorizing Official (AO).	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-70, 800-128; OMB Memo: M-07-11, M-07-18, M-08-22; Web: checklists.nist.gov, nsa.gov, nvd.nist.gov; IRS1075; CJIS 5.6	AC-19, CM-2, CM-3, CM-7, CM-8, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records. Examine: Information systems are configured to baselines: - Only approved operating systems are found; - Only approved deviations are found; and - Monitors configuration on a regular basis. Interview: Organizational personnel with security configuration responsibilities.	

CM-06(01): AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information system components. **CMS-ARS:** The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information system components as defined in the US HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance. Std.2 - Information system automated central management systems must be verified to meet system mission and user requirements.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-100; HHS: Minimum Security Configuration Standards for Departmental Operating Systems and Applications	CA-7, CM-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.	

Test: Automated mechanisms implementing the centralized management, application, and verification of configuration settings.

CM-06(02): RESPOND TO UNAUTHORIZED CHANGES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization responds to unauthorized changes to information system and components (e.g., authorization, auditing, processing types, baselines) and data (e.g., system libraries, log files, executables) in the following ways: a. Alert responsible actors (person, organization); b. Restore to approved configuration; and c. Halt system processing as warranted.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in the extreme case, halting affected information system processing.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	IR-4, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing configuration settings for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records. Test: Automated mechanisms implementing responses to unauthorized changes to configuration settings.	

CM-07: LEAST FUNCTIONALITY

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of high-risk system services, ports, network protocols, and capabilities (e.g., Telnet, FTP, etc.) across network boundaries that are not explicitly required for system or application functionality. **CMS-ARS, CMS-MARS-E:** c. A list of specifically needed system services, ports, and network protocols must be maintained and documented in the applicable security plan; all others will be disabled. **IRS:** b. Prohibit or restrict the use of the functions, ports, protocols, or services as defined in Office of Safeguards–approved compliance requirements (e.g., SCSEMs, assessment tools). c. Review the information system as part of vulnerability assessments to identify unnecessary or non-secure functions, ports, protocols, and services (see Section 9.3.14.3, Vulnerability Scanning (RA-5)). d. Disable defined functions, ports, protocols, and services within the information system deemed to be unnecessary or non-secure.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Automated configuration review results must be searchable by HHS Information Security:	

(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Configuration review information sources include systems, appliances, devices, services, and applications (including databases).
(c) HHS Information Security directed configuration review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by HHS, raw security information/results from automated periodic configuration review tools must be available in an unaltered format to HHS Information Security.
Std.3 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational configuration status and posture information.

CMS-MARS-E:
Std.4 The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: United States Government Configuration Baseline (USGCB)-defined list of prohibited or restricted functions, ports, protocols, and/or services.
Std.5 The organization shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available.

SUPPLEMENTAL GUIDANCE

Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., VoIP, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., USB, FTP, and HTTP) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; IRS-1075; CJIS 5.6	AC-6, CM-2, RA-5, SA-5, SC-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Examine: Information systems are configured to provide only the functionality necessary to perform mission.
Examples:
1. Networking minimizes functionality;
2. Privileged escalation mechanisms (tools) are properly configured;
3. Applications, including network protocols, are configured to maximize security; and
4. Firewall rules follow deny-all, permit-by-exception policy.
Examine: Information systems provide the capability to detect changes in configurations in an automated manner.
Test: Information system for disabling or restricting functions, ports, protocols, and services.

CM-07(01): PERIODIC REVIEW

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Reviews the information system no less often than annually to identify and eliminate unnecessary functions, ports, protocols, and/or services;
b. Disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure.

CMS-ARS:
a. Reviews the information system no less often than once every thirty (30) days to identify and eliminate unnecessary functions, ports, protocols, and/or services;
c. Performs automated reviews of the information system no less often than once every seventy-two (72) hours to identify changes in functions, ports, protocols, and/or services

CMS-MARS-E:
a. The organization reviews the information system at least quarterly to identify and eliminate unnecessary functions, ports, protocols, and/or services.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - Periodic configuration review results that are generated by automated tools must be searchable by HHS Information Security:
a. Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
b. Configuration review information sources include systems, appliances, devices, services, and applications (including databases); and
c. HHS Information Security directed configuration automated periodic review information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw security information/results from automated periodic configuration review tools must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	AC-18, CM-7, IA-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system configuration settings and associated documentation; security configuration checklists; and other relevant documents or records.
Examine: Information system provides the capability to identify changes in configurations in an automated manner.
Interview: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the information system.

CM-07(02): PREVENT PROGRAM EXECUTION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system prevents program execution in accordance with the list of authorized or unauthorized software programs and rules authorizing the terms and conditions of software program usage.

CMS-ARS:

The information system prevents program execution in accordance with policies regarding authorized software use which include, but are not limited to the following: a. Software must be legally licensed; b. Software must be provisioned in approved configurations; and c. Users must be authorized for software program use.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	CM-8, PM-5

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records. Test: Automated mechanisms preventing software program execution on the information system.

CM-07(03): REGISTRATION COMPLIANCE

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization ensures compliance with CJIS-defined registration requirements for functions, ports, protocols, and services.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functions, ports, protocols, and services.	

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; procedures addressing least functionality in the information system; configuration management plan; security plan; information system configuration settings and associated documentation; audit and compliance reviews; information system audit records; other relevant documents or records. Interview: Organizational personnel with information security responsibilities; system/network administrators. Test: Organizational processes ensuring compliance with registration requirements for functions, ports, protocols, and/or services; automated mechanisms implementing compliance with registration requirements for functions, ports, protocols, and/or services.

CM-07(04): UNAUTHORIZED SOFTWARE / BLACKLISTING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate	Overlay(s): CJIS, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
If software whitelisting is not implemented, the organization: a. Identifies defined software programs (defined in the applicable security plan) not authorized to execute on the information system;	

b. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system;
c. Reviews and updates the list of unauthorized software programs annually.

CMS-ARS:
c. Reviews and updates the list of unauthorized software programs no less often than every seventy-two (72) hours; and
d. Receives automated updates from a trusted source.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Low, Low Plus:
Std.1 - Either software whitelisting or software blacklisting must be implemented.
Std.2 - Automated unauthorized software/blacklisting tool results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Unauthorized software/blacklisting (and whitelisting when applicable) information sources include systems, appliances, devices, services, and applications (including databases);
(c) Unauthorized software/blacklisting information sources that do not support the exchange of information with HHS Information Security must be documented in the applicable risk assessment and security plan; and
(d) HHS Information Security directed unauthorized software/blacklisting information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.3 - As required by HHS, raw security information/results from automated unauthorized software/blacklisting tools must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7(5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution.

REFERENCES	RELATED CONTROLS
Federal: NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	CM-6, CM-8, PM-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records.
Interview: Organizational personnel with information security responsibilities; system/network administrators.
Test: Automated mechanisms preventing software program execution on the information system.

CM-07(05): AUTHORIZED SOFTWARE / WHITELISTING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS

The organization:
a. Identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system;
b. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system;
c. Reviews and updates the list of authorized software programs no less often than Annually.

CMS-ARS:
c. Reviews and updates the list of authorized software programs no less often than every seventy-two (72) hours; and
d. Receives automated updates from a trusted source.

CONTROL IMPLEMENTATION STANDARDS
CMS-ARS: Std.1 - An automated software whitelisting tool must be implemented. Std.2 - Authorized software whitelisting results must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Authorized software whitelisting (and blacklisting) information sources include systems, appliances, devices, services, and applications (including databases); (c) Authorized software whitelisting information sources that do not support the exchange of information with HHS Information Security must be documented in the applicable risk assessment and security plan; and (d) HHS Information Security directed unauthorized software whitelisting information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.3 - As required by HHS, raw security information/results from automated authorized software whitelisting tools must be available in an unaltered format to HHS Information Security.
SUPPLEMENTAL GUIDANCE
The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing least functionality in the information system; system security plan; information system design documentation; specification of preventing software program execution; information system configuration settings and associated documentation; and other relevant documents or records. Interview: Organizational personnel with information security responsibilities; system/network administrators. Test: Automated mechanisms preventing software program execution on the information system.

CM-08: INFORMATION SYSTEM COMPONENT INVENTORY

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Include all components within the authorization boundary of the information system; 3. Are at the level of granularity deemed necessary for tracking and reporting; and 4. Include: - Unique identifier and/or serial number; - Information system of which the component is a part; - Type of information system component (e.g., server, desktop, application); - Manufacturer/model information; - Operating system type and version/service pack level; - Presence of virtual machines; - Application software version/license information; - Physical location (e.g., building/room number); - Logical location (e.g., IP address, position with the IS architecture); - Media access control (MAC) address; - Ownership; - Operational status; - Primary and secondary administrators; and - Primary user.	

b. Reviews and updates the information system component inventory no less frequently than every 180 days for High systems or 365 days for Moderate, Low Plus, and Low systems, or per CM-8(1) and/or CM-8(2), as applicable.

IRS:
Additional requirements for maintaining a system component inventory are provided in Section 9.4.12, System Component Inventory, as well as NIST SP 800-70 Security Configuration Checklists Program for IT Products-Guidance for Checklists Users and Developers.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - All Government-owned equipment (i.e., servers, workstations, laptops, and other IT components) used to process, store, or transmit HHS information display an asset tag with a unique identifying asset number.
Std.2 - IT components with an asset tag are tracked in an asset inventory database to include (at a minimum) name, location, asset identification, owner, and description of use.
Std.3 - Fully integrate inventory of information system components with the organizational continuous monitoring capability (CM-7).
Std.4 - Automated asset inventory information tracking systems must:
(a) Transmit updates to HHS Information Security no less often that once every 72 hours.
Std.5 - Automated component tracking and management tool results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Authorized component information sources include systems, platforms, appliances, devices;
(c) Component information sources that do not support the exchange of information with HHS Information Security must be documented in the applicable risk assessment and security plan; and
(d) HHS Information Security directed authorized component information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - As required by HHS, raw security information/results from component tools must be available in an unaltered format to HHS Information Security.
Std.7 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational component status and posture information.
Std.8 - The organization must create and maintain the inventory of high value assets associated with the system.
(a) The inventory must identify other systems from which controls are inherited.

CMS-MARS-E:
Std.1 The organization defines information deemed necessary to achieve effective property accountability
Std.2 The organization establishes, maintains, and updates, within every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII).

SUPPLEMENTAL GUIDANCE

Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-2; HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iii); NIST SP: 800-37, 800-39, 800-128, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	CM-2, CM-6, PM-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system inventory records; and other relevant documents or records. Examine: Information systems and components managed within organizational automated inventory management capability. Test: Organizational processes for updating inventory of information system components; automated mechanisms implementing updating of the information system component inventory.

CM-08(01): UPDATES DURING INSTALLATIONS / REMOVALS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Identifying any changes or updates to system inventories allow organizations to accurately track the equipment on which their information systems are run and maintains an accurate inventory of hardware and software used to collect and manage PHI. Maintaining a current inventory supports accountability controls and may also support breach response efforts.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; and other relevant documents or records. Interview: Organizational personnel with information system installation and inventory responsibilities.	

CM-08(02): AUTOMATED MAINTENANCE

Priority: P1	
Baseline(s): High	CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2(2) for organizations that chooses to combine information system component inventory and baseline configuration activities.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-16-04	SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	

ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; and other relevant documents or records. Test: Automated mechanisms implementing information system component inventory management.

CM-08(03): AUTOMATED UNAUTHORIZED COMPONENT DETECTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Employs automated mechanisms no less than monthly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and b. Takes the following actions when unauthorized components and/or provisioned configurations are detected: 1. Disable access to the identified component; 2. Disable the identified component's network access; 3. Isolate the identified component; and 4. Notify the responsible actor (i.e., person/organization defined in security plan). **CMS-ARS, CMS-MARS-E:** a. Employs automated mechanisms no less than weekly to detect the presence of unauthorized hardware, software, and firmware components within the information system; and	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - All components within the system authorization boundary must be monitored in compliance with information security continuous monitoring (ISCM) requirements. **CMS-ARS (Cloud)**: Std.1 - For cloud service providers, this Standard replaces the above Enhancement. The organization: (a) Employs automated mechanisms to scan continuously, using automated mechanisms with a maximum five-minute delay in detection to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials. **CMS-MARS-E:** Std.1 - In a shared computing facility, the service provider employs automated mechanisms to scan continuously, using automated mechanisms with a maximum (5) five-minute delay in detection to detect the addition of unauthorized components/devices into the information system. Std.2 - In a shared computing facility, the service provider disables network access by such components/devices or notifies designated organizational officials.	
SUPPLEMENTAL GUIDANCE	
This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AC-17, AC-18, AC-19, CA-7, CM-8, RA-5, SI-3, SI-4, SI-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system design documentation;

information system inventory records; component installation records; change control records; and other relevant documents or records. Test: Automated mechanisms for detecting unauthorized components/devices on the information system.

CM-08(04): ACCOUNTABILITY INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization includes in the information system component inventory information, a means for identifying by position and role, and individuals responsible/accountable for administering those components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach or compromise, component needs to be recalled/replaced, or component needs to be relocated).	
REFERENCES	**RELATED CONTROLS**
OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system inventory records; component installation records; and other relevant documents or records.	

CM-08(05): NO DUPLICATE ACCOUNTING OF COMPONENTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing information system component inventory; system security plan; information system inventory records; component installation records; and other relevant documents or records. Interview: Organizational personnel with information system inventory responsibilities; organizational personnel with responsibilities for defining information system components within the authorization boundary of the system.	

CM-09: CONFIGURATION MANAGEMENT PLAN

Priority: P1

Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying and managing configuration items throughout the system development life cycle (SDLC); c. Defines the configuration items for the information system; d. Places the configuration items under configuration management; and e. Protects the configuration management plan from unauthorized disclosure and modification.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; NIST SP: 800-128; IRS1075; CJIS 5.6	CM-2, CM-3, CM-4, CM-5, CM-8, SA-10
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Configuration management policy; configuration management plan; procedures addressing configuration management planning; system security plan; and other relevant documents or records.	

CM-10: SOFTWARE USAGE RESTRICTIONS

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
CONTROL IMPLEMENTATION STANDARDS	

SUPPLEMENTAL GUIDANCE	
Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy; IS-AUP **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; IRS1075; CJIS 5.6	AC-17, CM-8, SC-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; and other relevant documents or records. Interview: Organizational personnel with software installation responsibilities; organizational personnel with responsibilities for managing software site licenses; organizational personnel responsible for monitoring peer-to-peer file-sharing technology.	

CM-10(01): OPEN SOURCE SOFTWARE

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS, IRS, CMS-MARS-E
CONTROL REQUIREMENTS	
a. The organization establishes restrictions on the use of open source software. Open source software must: 1. Be legally licensed 2. Be approved by the agency information technology department 3. Adhere to a secure configuration baseline checklist from the U.S. Government or industry	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; and other relevant documents or records. Interview: Organizational personnel with software installation responsibilities; organizational personnel with responsibilities for managing software site licenses; organizational personnel responsible for monitoring peer-to-peer file-sharing technology.	

CM-11: USER-INSTALLED SOFTWARE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes policies governing the installation of software by users; b. Enforces software installation policies through technical methods; and c. Monitors policy compliance at monthly intervals.	

IRS: b. Enforce software installation policies through automated methods c. Monitor policy compliance on a continual basis **CMS-ARS:** a. Prohibits the installation of software by users on all Government Funded Equipment (GFE);
CONTROL IMPLEMENTATION STANDARDS
CMS-ARS: Low, Low Plus, Moderate: Std.1 - Monitoring for user-installed software must be in compliance with information security continuous monitoring (ISCM) requirements. High: Std.2 - Whitelisting applications must prevent un-authorized user-installed software. Moderate & Low: Std.1 - Monitoring for user-installed software must be in compliance with information security continuous monitoring (ISCM) requirements.
SUPPLEMENTAL GUIDANCE
If provided the necessary privileges, users have the ability to install software in organizational information systems. To maintain control over the types of software installed, organizations identify permitted and prohibited actions regarding software installation. Permitted software installations may include, for example, updates and security patches to existing software and downloading applications from organization-approved "app stores." Prohibited software installations may include, for example, software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** CMS-ARS; CJIS 5.6; FedRAMP Rev. 4 Baseline; IRS1075	AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Software use policy, contract agreements, site licenses, software installation policy and procedures, file sharing policy, security plan; and other relevant documents or records.

(CP) CONTINGENCY PLANNING

The HHS organization establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for HHS information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CP-01: CONTINGENCY PLANNING POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	

2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
b. Reviews and updates (as necessary) the current:
1. Contingency planning policy at least every three (3) years or as necessitated by significant change.
2. Contingency planning procedures at least once every three hundred sixty five (365) days or as necessitated by significant change.

CMS-MARS-E:
b.1. Contingency planning policy at least every three hundred sixty-five (365) days or as necessitated by significant change.

CONTROL IMPLEMENTATION STANDARDS

State organizations shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimized, and the state organization will be able either to maintain or quickly resume mission-critical functions.

IRS:
All FTI that is transmitted to agencies is backed up and protected within IRS facilities. As such, the focus of contingency planning controls is on the protection of FTI stored in backup media or used at alternative facilities and not focused on the availability of data. Agencies must develop applicable contingencies for ensuring that FTI is available, based upon their individual risk-based approaches.

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PII:
Contingency planning policy and procedures must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(7)(i); NIST SP: 800-12, 800-34, 800-100; IRS1075; CJIS 5.6	PM-9

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy and procedures; other relevant documents or records.
Interview: Organizational personnel with contingency planning responsibilities.

CP-02: CONTINGENCY PLAN

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops a contingency plan for the information system in accordance with NIST SP 800-34 that:
1. Identifies essential HHS missions and business functions and associated contingency requirements;
2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential HHS missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by designated officials within the organization.
b. Distributes copies of the contingency plan to the ISO, Information Owner(s)/Custodian(s), and other stakeholders identified within the contingency plan;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system within the requirements outlined in implementation Std.3;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to key contingency personnel, system administrator, database administrator, and other personnel/roles as appropriate and organizational elements identified above; and
g. Protects the contingency plan from unauthorized disclosure and modification.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The plan shall be distributed to key personnel and a copy stored offsite.
Std.2 - Elements of the plan for information resources shall include:

a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:
   1. Mission-Critical Information Resources (specific system resources required to perform critical functions) to include:
      A. Internal and external points of contact for personnel that provide or receive data or support interconnected systems.
      B. Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.
   2. Disruption impacts and allowable outage times to include:
      A. Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.
      B. Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.
   3. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:
      A. Preventive controls and processes such as backup power, excess capacity, environmental sensors and alarms.
      B. Recovery techniques and technologies such as backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.
c. Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan.
d. Disaster Recovery Plan--Each state organization shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:
   1. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
   2. Identify recovery resources and a source for each;
   3. Contain step-by-step implementation instructions;
   4. Include provisions for annual testing.

Std.3 – The contingency plan for the information system should be reviewed and updated (if necessary) every three hundred and sixty five days as part of the annual risk assessment. See CP-4, Contingency Plan Testing for testing requirements.

CMS-ARS:
Std.4 - The system must be continuously monitored and assessed to ensure that it is operating as intended and that changes do not have an adverse effect on system performance.
Std.5 - The organization must verify that the provisioned implementation being assessed and/or monitored meets users' documented requirements and is an approved system configuration.

CSP:
Moderate & Low:
Std.4 - For cloud service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to which to distribute the CP. The contingency list includes designated FedRAMP personnel.
Std.5 - For cloud service providers, the organization defines a list of key contingency personnel (identified by name and/or by role) and organizational elements to communicate any CP changes to. The contingency list includes designated FedRAMP personnel.

CMS-MARS-E:
Std. - The system owner defines a list of key contingency personnel (identified by name and/or by role) and organizational elements for distribution and receipt of the contingency plan and any contingency plan changes. The contingency list includes designated HHS personnel.

SUPPLEMENTAL GUIDANCE

Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are impacted. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident.

PII:
Contingency plans must take privacy-applicable requirements into account so that executing contingency measures does not result in avoidable privacy incidents and breaches.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-3; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C), 45 C.F.R. §164.308(a)(7)(ii)(E), 45 C.F.R. §164.308(a)(7)(i)-(ii); 45 C.F.R. §164.310(a)(2)(i); 45 C.F.R. §164.312(a)(2)(ii); Homeland Security Presidential Directive (HSPD) 7: G(22)(i); NIST SP: 800-34; IRS1075	AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; and other relevant documents or records.
Examine: CFACTS to ensure contingency contact information is being maintained.
Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities.

CP-02(01): COORDINATE WITH RELATED PLANS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization coordinates contingency plan development with organizational elements responsible for related plans.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans (COOP), Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas.

CP-02(02): CAPACITY PLANNING

Priority: P1	
Baseline(s): High	CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber-attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; capacity planning documents; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities.

CP-02(03): RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-34; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities.	

CP-02(04): RESUME ALL MISSIONS / BUSINESS FUNCTIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization plans for the resumption of all missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-34	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities.	

CP-02(05): CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization plans for the continuance of Primary Mission Essential Functions (PMEF) with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites).	

PHI: Pursuant to the emergency mode operations plan and emergency access procedure mandated under HIPAA, this control is required for both provision of emergency services (a mission critical business function), and for protection of the security of PHI while operating in emergency mode.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-34; 45 C.F.R. §164.308(a)(7)(ii)(C); 45 C.F.R. §164.312(a)(2)(ii)	PE-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities.	

CP-02(08): IDENTIFY CRITICAL ASSETS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization identifies information system assets supporting essential missions and business functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. PHI: This control addresses the HIPAA Security Rule requirement to assess the relative criticality of specific applications and data to facilitate a risk-based contingency plan. Under HIPAA, this is an addressable control. The decision to implement this control is dependent on a risk analysis to determine if or to what extent it should be applied within the organization.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-34, 800-60; 45 C.F.R. §164.308(a)(7)(ii); CJIS 5.6	SA-14, SA-15
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; system security plan; business impact assessment; other related plans; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities.	

CP-03: CONTINGENCY TRAINING

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization provides contingency training to operational and support personnel (including managers and information system users) consistent with assigned roles and responsibilities: a. Within ninety (90) days of assuming a contingency role or responsibility; b. When required by information system changes; and c. Within every three hundred sixty-five (365) days thereafter.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Managers responsible for contingency operations and technical personnel should meet, at a minimum, once a year for review of contingency policies and procedures. Each review session should be documented and confirm that appropriate training has been completed.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(D); HSPD 7: G(22)(i); NIST SP: 800-16, 800-50; IRS1075	AT-2, AT-3, CP-2, IR-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; system security plan; contingency training records; and other relevant documents or records. Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.	

CP-03(01): SIMULATED EVENTS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: HSPD 7: G(22)(i)	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; and other relevant documents or records. Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.

CP-04: CONTINGENCY PLAN TESTING

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Tests the contingency plan for the information system in accordance with Implementation Std 2 using HHS-defined tests and exercises, such as the tabletop test to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed. **CMS-ARS:** a. Tests the contingency plan for the information system in accordance with Implementation Std 2 using NIST (NIST SP 800-34, NIST SP 800-84) and HHS-defined tests and exercises, such as the tabletop test, in accordance with the current HHS contingency plan procedure to determine the effectiveness of the plan and the organizational readiness to execute the plan;	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – A formal test need not be conducted if the organization actively exercises its contingency plan capability during real contingencies. Std.2 – Refer to the contingency plan for testing requirements. **IRS, CMS-MARS-E, CMS-ARS, VA:** Std.2 - Within every three hundred sixty-five (365) days **CMS-ARS:** CSP: Moderate & Low: Std.2 - Contingency plan test results will be made available to the HHS Information Owner(s)/Custodian(s) and all system developers and maintainers deployed within the CSP environment. Std.3 - For cloud service providers, the organization tests and/or exercises the contingency plan for the information system at least every 365 days using functional exercises to determine the plan's effectiveness and the organization's readiness to execute the plan. **CMS-MARS-E:** Std.1 - The organization must produce an after-action report to improve existing processes, procedures, and policies.	
SUPPLEMENTAL GUIDANCE	
Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans, including, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. PHI: Contingency plan tests and exercises should include an evaluation of the ability to meet privacy requirements in a contingency scenario as well as corrective measures to address any privacy risks identified. Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog	CP-2, CP-3, IR-3

Federal: IRS1075	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; system security plan; contingency plan testing and/or exercise documentation; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises.

CP-04(01): COORDINATE WITH RELATED PLANS

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization coordinates contingency plan testing with organizational elements responsible for related plans.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope:
1. Continuity of Operations Plan (COOP)
2. Business Continuity Plan (BCP)
3. Critical Infrastructure Protection (CIP) Plan
4. Disaster Recovery Plan (DRP)
5. Information System Contingency Plan (ISCP)
6. Cyber Incident Response Plan
7. Occupant Emergency Plan (OEP)

SUPPLEMENTAL GUIDANCE

Plans related to contingency plans for organizational information systems include, for example, BCPs, DRPs, COOPs, Crisis Communications Plans, CIP Plans, Cyber Incident Response Plans, and OEPs. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements.
Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope:
1. COOP
2. BCP
3. CIP Plan
4. DRP
5. ISCP
6. Cyber Incident Response Plan
7. OEP

REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: G(22)(i); NIST SP: 800-34	IR-8, PM-8

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; and other relevant documents or records.
Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; and organizational personnel with responsibilities for related plans.

CP-04(02): ALTERNATE PROCESSING SITE

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization tests the contingency plan at the alternate processing site: a. To familiarize contingency personnel with the facility and available resources; and b. To evaluate the capabilities of the alternate processing site to support contingency operations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: HSPD 7: G(22)(i)	CP-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records.	

CP-04(04): FULL RECOVERY / RECONSTITUTION

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	CP-10, SC-24
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records. Interview: Organizational personnel with information system recovery and reconstitution responsibilities; and organizational personnel with contingency plan testing and/or exercise responsibilities.	

CP-06: ALTERNATE STORAGE SITE

Priority: P1	
Baseline(s): Low Plus, Moderate, high	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes an alternate storage site, including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	

IRS: b. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Mission-critical information shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized state organization representatives.	
SUPPLEMENTAL GUIDANCE	
Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i); NIST SP: 800-34; IRS1075; CJIS 5.6	CP-2, CP-7, CP-9, CP-10, MP-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; and other relevant documents or records.	

CP-06(01): SEPARATION FROM PRIMARY SITE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; and other relevant documents or records.	

CP-06(02): RECOVERY TIME / POINT OBJECTIVES

Priority: P1

Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; and other relevant documents or records.	

CP-06(03): ACCESSIBILITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; mitigation actions for accessibility problems to the alternate storage site; and other relevant documents or records.	

CP-07: ALTERNATE PROCESSING SITE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes an alternate processing site, including necessary agreements to permit the transfer and resumption of information system operation types defined by HHS for essential missions/business functions within an allowable outage time as specified by the system contingency plan or COOP for the business function(s) supported by the system when the primary processing capabilities are unavailable;	

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

CMS-MARS-E:
a. The organization establishes an alternate processing site as well as the necessary agreements to permit the transfer and resumption of information system operations for essential missions/business functions within the time period specified in Implementation Std.1 when the primary processing capabilities are unavailable.

IRS:
The agency must:
c. Ensure that the alternate storage site provides information security safeguards that meet the minimum protection standards and the disclosure provisions of IRC 6103

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
CSP:
Moderate:
Std.1 - For cloud service providers, the organization defines a resumption time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the JAB.

CMS-MARS-E:
Std.1 - Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within a resumption time period consistent with the recovery time objectives defined by the business owner in the contingency plan.

SUPPLEMENTAL GUIDANCE

Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems.
Equipment and supplies required to resume operations within the HHS-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with HHS recovery time objectives.

PHI:
When an alternate processing site is used, administrative, physical and technical controls must be implemented to protect PHI in accordance with the organization's risk analysis.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(a)(2)(i), 45 C.F.R. §164.308(7)(ii)(C); NIST SP: 800-34; PPD-21; IRS1075; CJIS 5.6	CP-2, CP-6, CP-8, CP-9, CP-10, MA-6

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; system security plan; spare equipment and supplies at alternate processing site; equipment and supply contracts; service level agreements; and other relevant documents or records.

CP-07(01): SEPARATION FROM PRIMARY SITE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber-attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites is less relevant.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; and other relevant documents or records.	

CP-07(02): ACCESSIBILITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; and other relevant documents or records.	

CP-07(03): PRIORITY OF SERVICE

Priority: P1	
Baseline(s): Moderate, high	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organizational availability requirements (including recovery time objectives).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; and other relevant documents or records.	

CP-07(04): PREPARATION FOR USE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization prepares the alternate processing site so the site is ready to be used as the operational site supporting essential CMS missions and business functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place.	
REFERENCES	**RELATED CONTROLS**
	CM-2, CM-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; and other relevant documents or records. Test: Information system at the alternate processing site.	

CP-08: TELECOMMUNICATIONS SERVICES

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential HHS missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	
CONTROL IMPLEMENTATION STANDARDS	
Low Plus, Moderate: Std.1 - Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD). High: Std.1 - Ensure alternate telecommunications Service Level Agreements (SLA) are in place to permit resumption of system Recovery Time Objectives (RTO) and business functions Maximum Tolerable Downtimes (MTD). Std.2 - Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.	
SUPPLEMENTAL GUIDANCE	

This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-3; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B); NIST SP: 800-34; Web: tsp.ncs.gov	CP-2, CP-6, CP-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; system security plan; primary and alternate telecommunications service agreements; list of essential missions and business functions; and other relevant documents or records	

CP-08(01): PRIORITY OF SERVICE PROVISIONS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and b. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; and other relevant documents or records.	

CP-08(02): SINGLE POINTS OF FAILURE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.	
CONTROL IMPLEMENTATION STANDARDS	

Std.1 - The alternate telecommunication services provider must be separate from the primary service providers	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.	

CP-08(03): SEPARATION OF PRIMARY / ALTERNATE PROVIDERS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization obtains alternate telecommunications services from providers that are separated from primary service providers so as not to be susceptible to the same hazards.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers.	

CP-08(04): PROVIDER CONTINGENCY PLAN

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Requires primary and alternate telecommunications service providers to have contingency plans; b. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and c. Obtains evidence of contingency testing/training by providers within every 365 days.	
CONTROL IMPLEMENTATION STANDARDS	

SUPPLEMENTAL GUIDANCE	
Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with DHS and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training. CMS-ARS-3.0 Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with DHS and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.	
REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; and other relevant documents or records. Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers.

CP-09: INFORMATION SYSTEM BACKUP

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; c. Conducts backups of information system documentation, including security-related documentation and other forms of data, including paper records within the defined frequency (defined in the applicable security plan) consistent with recovery time and recovery point objectives; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations. **IRS:** d. Protect the confidentiality of backup information at storage locations pursuant to IRC 6103 requirements	
CONTROL IMPLEMENTATION STANDARDS	
Low, Low Plus: Std.1 - Perform backups of user-level and system-level information (including system state information) a minimum of monthly. Std.2 - Backups must be compliant with HHS requirements for protecting data at rest. (see SC-28) Moderate, High: Std.1 - Perform the following backups to include user-level and system-level information (including system state information): a. Full backups weekly to separate media. b. Incremental or differential backups daily to separate media. **HIPAA**: Std.5- Establish procedures that create a retrievable, exact copy of the PHI before any movement of information system equipment.	

CMS-ARS, CMS-MARS-E:
Std.2 - Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time, and action.

CMS-ARS:
Std.3 - Backups must be compliant with HHS requirements for protecting data at rest. (see SC-28)
Std.4 - Backup and recovery processes for all HHS information systems and resources must be documented and periodically reviewed by the agency IRM (or designee) or the CIO (or designee).

PII:
Std.6 - Ensure that a current, retrievable, copy of personally identifiable information (PII) is available before movement of servers.
Std.7 - Use the encryption methodology specified in SC-13 to encrypt personally identifiable information (PII) confidentiality impact level information in backups at the storage location.

Cloud:
Std 8 - The system owner shall determines what elements of the cloud environment requirement the Information System Backup control
Std.9 - The system owner determines how Information System Backup will be verified and the appropriate periodicity of the check

CJIS:
The metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

SUPPLEMENTAL GUIDANCE

System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information.
The transfer rate of backup information to an alternate storage site (if so designated) is guided by the HHS recovery time objectives and recovery point objectives. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time.

PII:
Backup copies of information need to be protected with the same level of security as if that information were being maintained on the original information system. Applicable controls necessary to achieve this and to protect confidentiality include encryption of the backup. Backing up information helps maintain the integrity of the data—a requirement of the Privacy Act and HIPAA.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** IRS1075; CJIS Security Policy; FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 45 C.F.R. §164.310(d)(2)(iv), 164.312(c)(1), 45 C.F.R. §164.308(a)(7)(ii)(C); NIST SP: 800-34; CJIS 5.6	CP-2, CP-6, MP-4, MP-5, SC-13, SC-28

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; backup storage location(s); information system backup logs or records; and other relevant documents or records.
Interview: Organizational personnel with information system backup responsibilities.

CP-09(01): TESTING FOR RELIABILITY / INTEGRITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization tests backup information in accordance with implementation Std 1 to verify media reliability and information integrity.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The organization tests the backup information of critical information systems at least annually and of non-critical systems using a risk based approach. Std.2 - A formal test need not be conducted if the organization completed a real world restore of the information system during the year. **CMS-MARS-E:** Std.1 - The organization tests backup information at least annually. **CMS-ARS:** Low, Low Plus: Std.1 - Backups are tested at least annually. Moderate: Std.1 - Backups are tested at least every six (6) months. High: Std.1 - Backups are tested at least every three (3) months.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CMS-ARS; FedRAMP Rev. 4 Baseline	CP-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; information system backup test results; backup storage location(s); and other relevant documents or records.	

CP-09(02): TEST RESTORATION USING SAMPLING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	CP-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan testing and/or exercise documentation; contingency plan test results; and other relevant documents or records.	

CP-09(03): SEPARATE STORAGE FOR CRITICAL INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	CM-2, CM-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); and other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information system backup responsibilities.	

CP-09(05): TRANSFER TO ALTERNATE STORAGE SITE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization transfers information system backup information to the alternate storage site at defined time periods (defined in the applicable security plan) and transfer rates (defined in the applicable security plan) consistent with the recovery time and recovery point objectives.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; system security plan; information system backup test results; alternate site service agreements; backup storage location(s); and other relevant documents or records.	

CP-10: INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
CONTROL IMPLEMENTATION STANDARDS
Std.1 - Recovery of the information system after a failure or other contingency must be done in a trusted, secure, and verifiable manner. Std.2 - Secure information system recovery and reconstitution may include, but is not limited to: (a) Reset all system parameters (either default or organization-established); (b) Reinstall patches; (c) Reestablish configuration settings; (d) Reinstall application and system software; and (e) Test the system.
SUPPLEMENTAL GUIDANCE
Recovery is executing information system contingency plan activities to restore HHS missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. PII: Information system recovery and reconstitution is an important step to restoring sensitive information, such as both personally identifiable information (PII) and protected health information (PHI), to an accurate state following execution of a contingency plan.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(7)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(C); HSPD 7: G(22)(i); NIST SP: 800-34; IRS1075; CJIS 5.6	CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; and other relevant documents or records. Test: Automated mechanisms and/or manual procedures for implementing information system recovery and reconstitution operations.

CP-10(02): TRANSACTION RECOVERY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements transaction recovery for systems that are transaction-based.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-34; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; contingency plan test results; and other relevant documents or records. Test: Automated mechanisms implementing transaction recovery capability.

CP-10(04): RESTORE WITHIN TIME PERIOD

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization provides the capability to restore information system components within the target restoration time period from configuration-controlled and integrity-protected information representing a known, operational state for the components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Restoration of information system components includes, for example, reimaging which restores components to known, operational states.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-34	CM-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Interview: Organizational personnel with information system recovery and reconstitution responsibilities.	

CP-11: ALTERNATE COMMUNICATIONS PROTOCOLS

Priority: P1	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The information system provides the capability to employs organization-defined alternative communications protocols in support of maintaining continuity of operations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Contingency plans and the associated training and testing for those plans, incorporate an alternate communications protocol capability as part of increasing the resilience of organizational information systems. Alternate communications protocols include, for example, switching from Transmission Control Protocol/Internet Protocol (TCP/IP) Version 4 to TCP/IP Version 6. Switching communications protocols may affect software applications and therefore, the potential side effects of introducing alternate communications protocols are analyzed prior to implementation.	
REFERENCES	**RELATED CONTROLS**
Federal: HIPAA Security Rule 45 C.F.R. § 164.308(a)(4)4	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Contingency planning policy; procedures addressing alternative communications protocols; contingency plan; continuity of operations plan; information system design documentation; information system configuration settings and associated documentation; list of alternative communications protocols supporting continuity of operations; other relevant documents or records. Interview: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with continuity of operations planning and plan implementation responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers. Test: Automated mechanisms employing alternative communications protocols.

(IA) IDENTIFICATION AND AUTHENTICATION

The HHS organization requires the identification of information system users, processes acting on behalf of users, or devices and authenticates (or verifies) the identities of those users, processes, or devices as a prerequisite to allowing access to HHS information systems.

IA-01: IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel that use HHS information resources 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. b. Reviews and updates (as necessary) the current: 1. Identification and authentication policy at least every three (3) years; and 2. Identification and authentication procedures at least once every three hundred sixty five (365) days) years. **CMS-MARS-E:** b.1. 1. Identification and authentication policy at least once every three hundred sixty five (365) days; and	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: EIS-Policy 10.8 **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-63, 800-73, 800-76, 800-78, 800-100; IRS1075; CJIS 5.6	PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Identification and authentication policy and procedures; other relevant documents or records. Interview: Organizational personnel with identification and authentication responsibilities.

IA-02: IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The HHS information system uniquely identifies and authenticates HHS organizational users (or processes acting on behalf of organizational users).	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. Std.2 - User identification shall be authenticated before the information resources system may grant that user access. **SPI:** Std.5 - Each member of the Applicant/Bidder's Workforce who will use, disclose, create, receive, transmit, or maintain HHS Confidential Information have a unique user name (account) and a private password. **CMS-MARS-E, CMS-ARS:** Std.3 - Require the use of system and/or network authenticators and unique user identifiers. Std.4 - Help desk support requires user identification for any transaction that has information security implications. **CMS-MARS-E:** Std.5 - For the information system uniquely identifying and authenticating organizational users (or processes acting on behalf of organizational users): Follow CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted VPNs for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government PIV card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8.	

PII: Implementing this control ensures unique identification of individual's account, preventing anonymous access to sensitive information such as personally identifiable information (PII) and providing appropriate access (e.g., need for the PII in the performance of the users official duties) for organizational users. HIPAA requires that organizations uniquely identify users and implement procedures to verify user identity.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy; Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2, 201; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D), 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); Homeland Security Presidential Directive (HSPD) -12; NIST SP: 800-63, 800-73, 800-76, 800-78; OMB Memo: M-04-04, M-06-16, M-11-11, M-16-04; Web: idmanagement.gov; IRS1075; CJIS 5.6	AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; and other relevant documents or records. Examine: Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Examples: 1. Privileged escalation mechanisms (tools) require authentication; and 2. Use of shared accounts, to include privileged accounts, is minimized or not used. Examine: Information system enforces approved multifactor authentication for network access to systems processing or storing CMS sensitive information. Test: Automated mechanisms implementing identification and authentication capability, to include strong authentication as required, for the information system. IA-2(1) Network Access to Privileged Accounts (High, Moderate, Low) (CSP: Mod, Low)	

IA-02(01): NETWORK ACCESS TO PRIVILEGED ACCOUNTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements multifactor authentication (MFA) for network access to privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication mechanisms must comply with the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04; CJIS 5.6	AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved multifactor authentication for network access to privileged accounts.	

Test: Automated mechanisms implementing identification and authentication capability for the information system.

IA-02(02): NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements multifactor authentication (MFA) for network access to non-privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication mechanisms must comply with the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved MFA for network access to non-privileged accounts. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(03): LOCAL ACCESS TO PRIVILEGED ACCOUNTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E, CJIS, VA
CONTROL REQUIREMENTS	
The information system implements multifactor authentication (MFA) for local access to privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication mechanisms must comply with the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04; CJIS 5.6	AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved MFA for local access to privileged accounts. Test: Automated mechanisms implementing identification and authentication capability for the information system. System and application management accounts need to be checked.	

IA-02(04): LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system implements MFA for local access to non-privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication mechanisms must comply with the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved MFA for local access to non-privileged accounts. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(05): GROUP AUTHENTICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; group identifiers; and other relevant documents or records. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(06): NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements multifactor authentication (MFA) for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device	

meets minimum token requirements discussed in the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card.	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved multifactor authentication for network access to privileged accounts that is compliant with CMS Authentication Standards. Test: Automated mechanisms supporting and/or implementing multifactor authentication capability. NOTE: System and application management accounts need to be checked.	

IA-02(07): NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements multifactor authentication (MFA) for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets minimum token requirements discussed in the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. PII: This control is required for remote network access to information systems containing personally identifiable information (PII) (from outside the organization controlled networks). A separate device could include a common access card (CAC).	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved MFA for network access to non-privileged accounts that is compliant with CMS Authentication Standards. Test: Automated mechanisms supporting and/or implementing MFA capability.	

IA-02(08): NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use cryptographic nonces (e.g., an arbitrary number that may only be used once such as an RSA token numeric) or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of privileged information system accounts; and other relevant documents or records. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(09): NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces (e.g., RSA token numeric) or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.	
REFERENCES	**RELATED CONTROLS**
Federal: HIPAA: 164.312(a)(2)(i); OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(11): REMOTE ACCESS - SEPARATE DEVICE

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements multifactor authentication for remote access to privileged accounts and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.	
CONTROL IMPLEMENTATION STANDARDS	
IRS: NIST SP 800-63 allows the use of software tokens **CMS-ARS, CMS-MARS-E:** Std.1 - The separate device must meet minimum token requirements discussed in the RMH, Volume III, Standard 3.1, CMS Authentication Standards. **CMS-MARS-E:** Std.2 - In reference to the information system implementing multifactor authentication for remote access to privileged and non-privileged accounts, assuring that one of the factors is provided by a device separate from the system gaining access: Reference CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. PII: A separate device could include a personal identity verification (PIV) card. This control is required when the network access is remote (from outside the organization controlled networks).	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; HSPD-12; OMB Memo: M-16-04; CJIS 5.6	AC-6, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; and other relevant documents or records. Examine: Information system enforces approved multifactor authentication for that is compliant with CMS Authentication Standards. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-02(12): ACCEPTANCE OF PIV CREDENTIALS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, VA
CONTROL REQUIREMENTS	
The information system accepts and electronically verifies PIV credentials.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). PIV credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AU-2, PE-3, SA-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Test: Automated mechanisms implementing PIV credential capability for the information system.

IA-02(13): OUT-OF-BAND AUTHENTICATION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system implements out-of-band authentication identified in Std.1 under out-of-band authentication is used as an advanced authentication method.

CONTROL IMPLEMENTATION STANDARDS

Std. 1 - Authenticator is sent on demand via text message, phone call, etc. (CJIS 5.6.2.2)

SUPPLEMENTAL GUIDANCE

Out-of-band authentication (OOBA) refers to the use of two separate communication paths to identify and authenticate users or devices to an information system. The first path (i.e., the in-band path), is used to identify and authenticate users or devices, and generally is the path through which information flows. The second path (i.e., the out-of-band path) is used to independently verify the authentication and/or requested action. For example, a user authenticates via a notebook computer to a remote server to which the user desires access, and requests some action of the server via that communication path. Subsequently, the server contacts the user via the user's cell phone to verify that the requested action originated from the user. The user may either confirm the intended action to an individual on the telephone or provide an authentication code via the telephone. This type of authentication can be employed by organizations to mitigate actual or suspected man-in the-middle attacks. The conditions for activation can include, for example, suspicious activities, new threat indicators or elevated threat levels, or the impact level or classification level of information in requested transactions.

REFERENCES	RELATED CONTROLS
Federal: HSPD-12; OMB Memoranda 04-04, 06-16, 11-11; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78; FICAM Roadmap and Implementation Guidance; Web: http://idmanagement.gov. ; CJIS 5.6	IA-10, IA-11, SC-37

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; system-generated list of out-of-band authentication paths; other relevant documents or records.
Interview: Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers.
Test: Automated mechanisms supporting and/or implementing out-of-band authentication capability.

IA-03: DEVICE IDENTIFICATION AND AUTHENTICATION

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system uniquely identifies and authenticates devices before establishing a remote connection.

IRS:
The information system uniquely identifies and authenticates devices before establishing a connection.

CMS-ARS, CMS-MARS-E:
The information system uniquely identifies and authenticates defined types of devices (defined in the applicable security plan) that require authentication mechanisms, which, at a minimum, use shared information (MAC or IP address) and access control lists to control remote network access, before establishing a connection that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - If remote authentication is provided by the system itself, the system must be in compliance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.

CMS-ARS, CMS-MARS-E:
Cloud:
Std.2 - For cloud service providers, this Standard replaces the above Control. The organization defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the JAB.

IRS:
Std.1 - Organizational devices requiring unique device-to-device identification and authentication may be defined by type, device, or a combination. Information systems typically use of the following to identify and authenticate:
a. Shared known information (e.g., MAC or IP address)
b. An organizational authentication solution (e.g., IEEE 802.1x and EAP, Radius server, Kerberos).

SUPPLEMENTAL GUIDANCE

Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or TCP/IP addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability.
Note: At a minimum, HHS information systems should be filtered by MAC and/or IP address when accessing remote systems.

PHI:
Implementing this control ensures that un-authenticated devices, e.g., mobile devices and personal laptop computers, are not able to make a connection to an information system containing PHI. HIPAA requires technical policies and procedures for systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(a)(1); IRS1075; CJIS 5.6	AC-17, AC-18, AC-19, CA-3, IA-4, IA-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; and other relevant documents or records. Test: Automated mechanisms implementing device identification and authentication.

IA-03(01): CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system authenticates devices when the connections must comply with CJIS Advanced Authentication requirements before establishing local, remote, or network connections using bidirectional authentication that is cryptographically based.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections).	
REFERENCES	**RELATED CONTROLS**
CJIS 5.6	SC-8, SC-12, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; list of devices requiring unique identification and authentication; device connection reports; information system configuration settings and associated documentation; other relevant documents or records. Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers. Test: Automated mechanisms supporting and/or implementing device authentication capability; cryptographically based bidirectional authentication mechanisms.	

IA-03(04): DEVICE ATTESTATION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization ensures that device identification and authentication based on attestation is handled by organization-defined configuration management process that is compliant with CJIS requirements.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; procedures addressing device identification and authentication; procedures addressing device configuration management; information system design documentation; information system configuration settings and associated documentation; configuration management records; change control records; information system audit records; other relevant documents or records. Interview: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators. Test: Automated mechanisms supporting and/or implementing device identification and authentication capability; automated mechanisms supporting and/or implementing configuration management; cryptographic mechanisms supporting device attestation.

IA-04: IDENTIFIER MANAGEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization manages information system identifiers by: a. Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for one year; e. Disabling the identifier after ninety (90) days of inactivity. **CMS-ARS:** d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three (3) years or more has passed; and e. Disabling the identifier after the following period of in activity: 30 days for High, 60 days for Moderate, or 90 days for Low and Low Plus systems. **CMS-MARS-E:** d. Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of two (2) years or more has passed; and e. The organization manages information system identifiers by disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the state organization change Std.2 - SSNs, and parts of SSNs, must not be used as system identifiers. Identifier management must ensure that any access to, or action involving, personally identifiable information (PII) is attributable to a unique individual. **CMS-ARS, CMS-MARS-E:** Cloud: Std.1 - For cloud service providers, the organization prevents reuse of user or device identifiers for at least two (2) years and disables the user identifier after ninety (90) days of inactivity. Std.2 - For cloud service providers, the organization defines time period of inactivity for device identifiers. The time period is approved and accepted by the JAB.	
SUPPLEMENTAL GUIDANCE	
Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers	

implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

PHI:
Identifier management must ensure that any access to, or action involving, PHI is attributable to a unique individual.

PII:
Identifiers are a critical and necessary function to confirm which people and devices are accessing sensitive information such as PII. Using SSNs as identifiers may create the potential for unauthorized disclosure of the SSN and linkage of that individual to other PII, as system identifiers are not protected with the same level of security as are database elements or passwords. In addition, collecting an individual's SSN may create notice requirements under the Privacy Act.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.312(a)(2)(i), 45 C.F.R. §164.312(d); 45 C.F.R. §164.308(a)(4); 45 C.F.R. §164.308(a)(5)(ii)(D); IRS1075; CJIS 5.6	AC-2, IA-2, IA-3, IA-5, IA-8, SC-37

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; and other relevant documents or records.
Interview: Organizational personnel with identifier management responsibilities.

IA-04(02): SUPERVISOR AUTHORIZATION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization requires that the registration process to receive an individual identifier includes supervisor authorization.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization requires that the registration process to receive an individual identifier includes supervisor authorization.

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.
Interview: Organizational personnel with identifier management responsibilities; supervisors responsible for authorizing identifier registration; organizational personnel with information security responsibilities; system/network administrators].
Test: Automated mechanisms supporting and/or implementing identifier management.

IA-04(03): MULTIPLE FORMS OF CERTIFICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Identity proofing registration process is mandatory for Federal Employees, Contractors, and Service Members.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization requires that multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; list of identifiers generated from physical access control devices; and other relevant documents or records. Interview: Organizational personnel with identifier management responsibilities.	

IA-04(04): IDENTIFY USER STATUS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization manages individual identifiers by uniquely identifying each individual such as contractors and foreign nationals.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AT-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) the organization defines the characteristic to be used to identify user status; and (ii) the organization manages user identifiers by uniquely identifying the user with the organization-defined characteristic identifying user status.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; list of characteristics identifying user status; and other relevant documents or records	

IA-05: AUTHENTICATOR MANAGEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization manages information system authenticators by:	

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators as follows:
- Passwords are valid for no longer than the period directed in IA-5(1), immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords);
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

IRS:
k. Password-protect system initialization (boot) settings

CMS-MARS-E, CMS-ARS:
g. Changing/refreshing authenticators as follows:
1. Passwords are valid for no longer than the period directed in IA-5(1);
2. Personal Identity Verification (PIV)-compliant access cards are valid for no longer than five (5) years; and
3. Public Key Infrastructure (PKI) certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years;
k. Password-protect system initialization (boot) settings

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Cloud:
Std.1 - For cloud service providers, the organization manages information system authenticators for users and devices by changing/refreshing authenticators every sixty (60) days by authenticator type.

SUPPLEMENTAL GUIDANCE

Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords.

PHI:
Under HIPAA, this is an addressable control.

PII:
Adequate security to ensure confidentiality for an information system containing sensitive information such as personally identifiable information (PII) is achieved through the management of the authenticators permitting access to that system. Authenticator management includes periodically changing passwords or other identifiers (e.g., certification and signatures) to reinforce identity validation and adherence to administrative security policies as well as enforces a time-based restriction on access, all of which bound access to PII in some way, limiting exposure in the event a user account is compromised.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); NIST SP: 800-63, 800-73, 800-76, 800-78; OMB Memo: M-04-04, M-11-11; Web: idmanagement.gov; 45 C.F.R. §164.308(a)(3); 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(d); IRS1075; CJIS 5.6	AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Assessment Methods and Objects:
Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for determining initial authenticator content.
Test: Automated mechanisms implementing authenticator management functions.

IA-05(01): PASSWORD-BASED AUTHENTICATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, Web & Mobile, DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

a. Meets or exceeds enforcement of the following minimum password complexity requirements:
- MinimumPasswordLength = Fifteen (15) characters for High or eight (8) characters for Moderate, Low-Plus and Low systems;
- PasswordComplexity = minimum (three (3) for High or one (1) for Moderate or Low) character(s) from the four (4) character categories
  - Upper case alpha (A-Z)
  - Lower case alpha (a-z)
  - Number (0-9)
  - Special characters (e.g. @#$%^%*()_+|~-=\?{}[]:?;?<>/)
- Prohibits the use of dictionary names or words

b. If the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at twelve (12) for High and four (4) for Moderate, Low-Plus or Low systems;
c. Stores and transmits only cryptographically-protected of passwords; and
d. Enforces password minimum and maximum lifetime restrictions of:
- MinimumPasswordAge = one (1) day;
- MaximumPasswordAge = sixty (60) days (privileged accounts), ninety (90) days (non-privileged accounts), one hundred eighty (180) days (system/service accounts);

e. Prohibit password reuse for twelve (12) generations for High or six (6) generations for Moderate, Low Plus or Low systems.
e. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

IRS:
d. Enforces password minimum and maximum lifetime restrictions of:
- MinimumPasswordAge = one (1) day;
- MaximumPasswordAge = sixty (60) days (privileged accounts), ninety (90) days (non-privileged accounts), sixty (60) days (system/service accounts);

e. Prohibit password reuse for twenty-four (24) generations

CMS-MARS-E:
For password-based authentication, the information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:

a. Meets or exceeds enforcement of the following minimum password complexity requirements:
- MinimumPasswordLength = eight (8) characters, fifteen (15) characters for processes acting on behalf of users (e.g. system/service accounts);
- PasswordComplexity = minimum (three (3) for High or one (1) for Moderate or Low) character(s) from the four (4) character categories
  - Upper case alpha (A-Z)
  - Lower case alpha (a-z)
  - Number (0-9)
  - Special characters (@#$%^%*()_+|~-=\?{}[]:?;?<>/)
- Prohibits the use of dictionary names or words (see implementation Std.1)

d. Enforces password minimum and maximum lifetime restrictions of:
- MinimumPasswordAge = one (1) day;
- MaximumPasswordAge = sixty (60) days (privileged accounts), sixty (60) days (non-privileged accounts), one-hundred eighty (180) days (processes acting on behalf of a user);

e. Prohibit password reuse for twenty-four (24) generations

CMS-ARS:
The information systems follow the direction in the applicable configuration baselines per CM-6, or as follows, whichever is more stringent:
a. Prohibits the use of dictionary names or words;
b. If the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at twelve (12) for High and six (6) for Moderate, Low-Plus or Low systems;
f. The minimum length (MinimumPasswordLength) for administrators or privileged users is fifteen (15) characters;

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Mobile devices are excluded from the password complexity requirement.

Web & Mobile:
Std.2 - User passwords must be stored using secure hashing techniques with strong algorithm (e.g. PBKDF2, bcrypt, scrypt). FIPS and NIST Special Publications specify a number of approved cryptographic algorithms.

CMS-ARS:
(Cloud):
Std.3 - For cloud service providers, this Standard replaces the above Enhancement. The information system, for password-based authentication: (a) Enforces minimum password complexity of case sensitive, minimum of twelve (12) characters, and at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters; (b) Enforces at least one (1) changed character or as determined by the information system (where possible) when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of one (1) day minimum, sixty (60) days maximum; and (e) Prohibits password reuse for twenty four (24) generations.
For cloud service providers, this Standard replaces the above Enhancement. When password authentication is used for any purpose (e.g., system access, data protection by any application), the information system, for password-based authentication.

SUPPLEMENTAL GUIDANCE

This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., PIV cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords.

Dictionary words refers to a password comprised of a single Upper/Lower case character word that can be found in a dictionary. Combinations of words (passphrases) and words with numbers and/or special characters are not dictionary words.

REFERENCES	RELATED CONTROLS
Texas HHS: Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog	IA-6

Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Test: Automated mechanisms implementing authenticator management functions.

IA-05(02): PKI-BASED AUTHENTICATION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system, for PKI-based authentication:
a. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b. Enforces authorized access to the corresponding private key;
c. Maps the authenticated identity to the account of the individual or group; and
d. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor, including certificate policy processing.

REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	IA-6

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; PKI certification revocation lists; and other relevant documents or records.
Interview: Organizational personnel with responsibilities for PKI-based authentication management.
Test: Automated mechanisms implementing PKI-based authenticator management functions.

IA-05(03): IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization requires that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be conducted in person before a designated registration authority with authorization by defined personnel or roles (defined in the applicable security plan).

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
(Cloud)
Std.1 - For cloud service providers, the organization requires that the registration process to receive HSPD-12 smart cards be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; and other relevant documents or records.
Interview: Organizational personnel with authenticator management responsibilities.

IA-05(04): AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

(Cloud)
The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy CMS password strength requirements.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Add-on capabilities will be used when password strength determination is not supported by the underlying technology.

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline	CA-2, CA-7, RA-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization:
(i) defines requirements to be satisfied by password authenticators; and
(ii) employs automated tools to determine if password authenticators are sufficiently strong to satisfy organization-defined requirements.

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; and other relevant documents or records.
Interview: Organizational personnel with authenticator management responsibilities. Interview: Organizational personnel with authenticator management responsibilities.

IA-05(05): CHANGE AUTHENTICATORS PRIOR TO DELIVERY

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components.

REFERENCES	RELATED CONTROLS
CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization requires developers/installers of information system components to: provide unique authenticators prior to delivery/installation; or change default authenticators prior to delivery/installation.
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for information system procurements or services; other relevant documents or records. Interview: Organizational personnel with authenticator management responsibilities; organizational personnel with information system security, acquisition, and contracting responsibilities; system developers. Test: Automated mechanisms supporting and/or implementing authenticator management capability.

IA-05(06): PROTECTION OF AUTHENTICATORS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
For information systems containing multiple security categories of information without reliable physical or logical separation between categories, authenticators used to grant access to the systems are protected commensurate with the highest security category of information on the systems.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization protects authenticators commensurate with the security category of the information to which use of the authentication permits access.
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; procedures addressing authenticator management; information classification or sensitivity documentation; security categorization documentation for the information system; security assessments of authenticator protections; risk assessment results; system security plan; and other relevant documents or records. Interview: Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections.

IA-05(07): NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS

Priority: P1	
Baseline(s):	Overlay(s): Web & Mobile, CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std.1 - Never allow credentials to be embedded directly within the application code. Std.2 - Embedding database credentials within source code is not acceptable.	
SUPPLEMENTAL GUIDANCE	
Organizations exercise caution in determining whether embedded or stored authenticators are in encrypted or unencrypted form. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).	

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Web & Mobile Standard **Federal:** FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; and other relevant documents or records.

IA-05(08): MULTIPLE INFORMATION SYSTEM ACCOUNTS

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.

CONTROL IMPLEMENTATION STANDARDS

Std. 1 - Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.
Std. 2 - Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

SUPPLEMENTAL GUIDANCE

When individuals have accounts on multiple information systems, there is the risk that the compromise of one account may lead to the compromise of other accounts if individuals use the same authenticators. Possible alternatives include, for example: (i) having different authenticators on all systems; (ii) employing some form of single sign-on mechanism; or (iii) including some form of one-time passwords on all systems.

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization defines security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems; and implements organization-defined security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.

ASSESSMENT METHODS AND OBJECTS

Examine: Identification and authentication policy; procedures addressing authenticator management; security plan; list of individuals having accounts on multiple information systems; list of security safeguards intended to manage risk of compromise due to individuals having accounts on multiple information systems; other relevant documents or records.
Interview: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators.
Test: Automated mechanisms supporting and/or implementing safeguards for authenticator management.

IA-05(11): HARDWARE TOKEN-BASED AUTHENTICATION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std. 1 - See RMH, Volume III, Standard 3.1, CMS Authentication Standards for further information

SUPPLEMENTAL GUIDANCE	
Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; and other relevant documents or records.	

IA-06: AUTHENTICATOR FEEDBACK

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The feedback from information systems does not provide information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of information systems or system components, for example, desktops/notebooks with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with 2-4 inch screens, this threat may be less significant, and may need to be balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring the feedback of authentication information includes, for example, displaying asterisks when users type passwords into input devices, or displaying feedback for a very limited time before fully obscuring it. PHI: Restricting feedback from the authentication process limits ability of unauthorized users to compromise the authentication mechanisms for accounts that can access PHI. Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R. §164.312(a)(1); IRS1075; CJIS 5.6	PE-18
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; system security plan; information system design documentation; information system configuration settings and associated documentation; application code reviews for authentication mechanisms; and other relevant documents or records. Interview: Organizational personnel with responsibility for authentication mechanisms.	

Test: Authentication mechanisms on all interfaces. Verify that each authentication mechanism obscures authentication information during input and/or authentication attempt. Determine whether the method used to obscure authentication information is appropriate for the information type and display location (see Supplemental Guidance).

IA-07: CRYPTOGRAPHIC MODULE AUTHENTICATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal/state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
CONTROL IMPLEMENTATION STANDARDS	
IRS: Std. 1 - Validation provides assurance that when agency implements cryptography to protect FTI, the encryption functions have been examined in detail and will operate as intended. All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/.	
SUPPLEMENTAL GUIDANCE	
Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. **CMS-ARS:** PHI: Under HIPAA, this is an addressable control. A FIPS 140-2 validated cryptographic module is required. PII: Information systems containing personally identifiable information (PII) must use FIPS 140-2 validated cryptographic modules.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 140; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(D); 45 C.F.R.§164.312(a)(2)(iv) Web: csrc.nist.gov/groups/STM/cmvp/index.html; IRS1075; CJIS 5.6	SC-12, SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; system security plan; information system design documentation; information system configuration settings and associated documentation; application code reviews for cryptographic module implementation and/or use; FIPS 140-2 validation certificate number(s) for implemented cryptographic module(s); and other relevant documents or records. Interview: Organizational personnel with responsibility for cryptographic mechanisms. Test: Authentication mechanisms on all cryptographic modules. Verify that each cryptographic module has a FIPS 140-2 validation certificate and is operating in the FIPS-approved mode of operation. Verify that all authentication mechanisms for each cryptographic module meet the requirements of all control-specified requirements.	

IA-08: IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - Follow CMS guidance provided in the Electronic Authentication Guidelines for ACA Administering Entity Systems, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ CMS-ARS: Std.1 - If E-Authentication is used, refer to Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards	
SUPPLEMENTAL GUIDANCE	
Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. PHI: Under HIPAA, this is an addressable control. PII: Similar to IA-2, this control requires information systems to uniquely identify and authenticate system users that are not part of the organization as well as processes that act on behalf of another organization. This means no one is provided anonymous access to sensitive information, such as personally identifiable information (PII), and supports managing each user's appropriate access to sensitive information.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State**: DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 201; NIST SP: 800-63, 800-116; OMB Memo: M-04-04, M-10-06-2011, M-11-11; Web: idmanagement.gov; 45 C.F.R. §164.312(a)(2)(i); IRS1075; CJIS 5.6	AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; and other relevant documents or records. Test: Automated mechanisms implementing identification and authentication capability for the information system.	

IA-08(01): ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, VA
CONTROL REQUIREMENTS	

The information system accepts and electronically verifies PIV credentials from federal agencies.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 201; CJIS 5.6	AU-2, PE-3, SA-4

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; PIV credential documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for PIV credential management.

IA-08(02): ACCEPTANCE OF THIRD-PARTY CREDENTIALS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, VA
CONTROL REQUIREMENTS	
The information system accepts only FICAM-approved third-party credentials.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the FICAM Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels.	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 201; CJIS 5.6	AU-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM credential documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for FICAM credential management.

IA-08(03): USE OF FICAM-APPROVED PRODUCTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, VA
CONTROL REQUIREMENTS	
The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users and accept third-party credentials.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the FICAM Conformance Program.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 201; CJIS 5.6	SA-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-approved information system component procedures; and other relevant documents or records. Interview: Organizational personnel with responsibilities for FICAM-approved information system component management.	

IA-08(04): USE OF FICAM-ISSUED PROFILES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, VA
CONTROL REQUIREMENTS	
The information system conforms to FICAM-issued profiles.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange).	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 201	SA-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Identification and authentication policy; procedures addressing authenticator management; system security plan; information system design documentation; information system configuration settings and associated documentation; FICAM-issued credential documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for FICAM-issued credential management.	

(IR) INCIDENT RESPONSE

The HHS organization (i) establishes an operational incident handling capability for HHS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) tracks, documents, and reports incidents to appropriate HHS and HHSC officials and/or authorities.

IR-01: INCIDENT RESPONSE POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls. b. Reviews and updates (as necessary) the current: 1. Incident response policy within every three (3) years; and 2. Incident response procedures within at least once every three hundred sixty five (365) days. **CMS-ARS:** PII: Applicable personnel (item a) include the Incident Response Team as required by OMB M-07-16. **CMS-MARS-E:** b.1. Incident response policies within at least once every three hundred sixty five (365) days.
CONTROL IMPLEMENTATION STANDARDS
Std.1 - State organizations shall assess the significance of a security incident based on the business impact on the affected resources and the current and potential technical effect of the incident, e.g., loss of revenue, productivity, access to services, reputation, unauthorized disclosure of confidential information, or propagation to other networks.
SUPPLEMENTAL GUIDANCE
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PHI: In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving PHI. PII: In developing incident response policy and procedures, ensure those policies and procedures incorporates guidance from the privacy office for the handling of incidents involving personally identifiable information (PII).

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-1, AS-2, SM-1, SM-3; HIPAA: 45 C.F.R.§164.308(a)(6)(i); 45 C.F.R. §164.530(b)(1); NIST SP: 800-12, 800-61, 800-83, 800-100; IRS1075; CJIS 5.6	PM-9, SE-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if: (i) The organization develops and documents incident response policy; (ii) The organization incident response policy addresses: - Purpose; - Scope; - Roles and responsibilities; - Management commitment; - Coordination among organizational entities; and - Compliance. (iii) The organization disseminates documented incident response policy to applicable personnel within the organization having associated incident response roles and

responsibilities;
(iv) The organization develops and documents incident response procedures;
(v) The organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls;
(vi) The organization disseminates documented incident response procedures to applicable personnel within the organization having associated incident response roles and
responsibilities; and
(vii) The organization reviews the incident response policy and procedures within every three hundred sixty-five (365) days, and updates them as necessary.

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response; system security plan; incident response plan; and other relevant documents or records.
Interview: Organizational personnel with incident response operational responsibilities.

IR-02: INCIDENT RESPONSE TRAINING

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within one (1) month of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

IRS:
Agencies must train personnel with access to FTI, including contractors and consolidated data center employees if applicable, in their incident response roles on the information system and FTI. The agency must provide incident response training to information system users consistent with assigned roles and responsibilities.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Formally tracks personnel participating in incident response training.

CMS-MARS-E:
Std.1 - The organization:
a. Identifies employees with significant information security responsibilities and provides role-specific training in accordance with NIST standards and guidance;
b. Includes user training in the identification and reporting of suspicious activities, both from external and internal sources;
c. Exposes all information systems users (i.e., employees, contractors, students, guest researchers, visitors, and others who may need access to information systems and applications) to security awareness materials addressing IR response associated with the roles. For example, regular users may only need to know whom to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration.
Std.2 - Provides information systems security refresher training for employees as frequently as determined necessary, based on the sensitivity of the information that the employees uses or processes and their role.

SUPPLEMENTAL GUIDANCE

Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

PII:
Those responsible for identifying and responding to a security incident must understand how to recognize when sensitive information such as personally identifiable information (PII) or protected health information (PHI) is involved so that they can coordinate with the designated (e.g., privacy) official.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; Federal Information Systems Controls Audit Manual (FISCAM): AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(6)(i); NIST SP: 800-16, 800-50; OMB Memo: M-16-04; IRS1075; CJIS 5.6	AT-3, CP-3, IR-8, AR-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization identifies personnel with incident response roles and responsibilities with respect to the information system;
(ii) The organization provides incident response training to information system users consistent with assigned roles and responsibilities;
(iii) Incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;
(iv) The organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training in accordance with organization-defined
frequency;
(v) The organization provides refresher incident response training in accordance with organization-defined frequency; and
(vi) The organization meets all the requirements specified in the applicable Implementation Standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response training; incident response training material; system security plan; incident response plan; incident response training records; and other relevant documents or records.
Examine: Information system includes capability to track participation in incident response training activities.
Interview: Organizational personnel with incident response training and operational responsibilities

IR-02(01): SIMULATED EVENTS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response training and incident response.
Interview: Organizational personnel with incident response training and operational responsibilities.

IR-02(02): AUTOMATED TRAINING ENVIRONMENTS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Examine: Incident response policy; procedures addressing incident response training; incident response training material; system security plan; incident response plan; incident response training records; and other relevant documents or records. Examine: Information system implements automated mechanisms to provide thorough and realistic incident response training environment. Interview: Organizational personnel with incident response training and operational responsibilities.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization employs automated mechanisms to provide a more thorough and realistic incident response training environment	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; automated mechanisms supporting incident response training; incident response plan; security plan; other relevant documents or records. Interview: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security responsibilities. Test: Automated mechanisms that provide a thorough and realistic incident response training environment.	

IR-03: INCIDENT RESPONSE TESTING

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
a. The organization tests the incident response capability for the information system within every three hundred sixty-five (365) days using NIST SP 800-61, reviews, analyses, and/or simulations to determine the incident response effectiveness and documents. **CMS-MARS-E:** b. Must produce an after-action report to improve existing processes, procedures, and policies; **IRS:** a. Agencies must perform tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures. b. A subset of all employees and contractors with access to FTI must be included in table top exercises. c. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies. See Section 10.3, Incident Response Procedures, for specific instructions on incident response requirements where FTI is involved.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - A formal test need not be conducted if the organization actively exercises its response capability during real incidents. **CMS-ARS:** Moderate & High Std.2 - Incident response capability tests must exercise (or simulate exercise of) all organizational response capabilities. The organization's documented response to an actual historic incident may be used as part of an incident response capability test, and any response capabilities that were not exercised as part of the historic incident response must be additionally exercised (or simulated) as part of the test. Cloud: Std.3 - For cloud service providers, the organization defines tests and/or exercises in accordance with NIST SP 800-61 (as amended).	

Std.4 - For cloud service providers, the organization provides test plans to FedRAMP at least every 365 days. Test plans are approved and accepted by the JAB prior to commencing testing.
SUPPLEMENTAL GUIDANCE
Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. If the organization routinely responds to incidents, and follows the documented incident response plan to do so, then full-scale simulations (or "table-top exercises") might not be necessary, especially if the documentation produced from the incident response is sufficient to provide a thorough understanding of the breadth and depth of the organization's analysis and response to the incident (including lessons learned). However, it is often the case that responses to incidents do not exercise the full incident response plan (for example, an incident might not meet the documented threshold requiring the organization to alert the Media about the incident). If the organization uses a historic response to an incident as the basis for the annual incident response capability test, any parts of the incident response capability that were not exercised in the historic response must be tested (either actually or through simulation) and documented as part of the capability test. Cloud: If the organization routinely responds to incidents, and follows the documented incident response plan to do so, then full-scale simulations (or "table-top exercises") might not be necessary, especially if the documentation produced from the incident response is sufficient to provide a thorough understanding of the breadth and depth of the organization's analysis and response to the incident (including lessons learned). However, it is often the case that responses to incidents do not exercise the full incident response plan (for example, an incident might not meet the documented threshold requiring the organization to alert the Media about the incident). If the organization uses a historic response to an incident as the basis for the annual incident response capability test, any parts of the incident response capability that were not exercised in the historic response must be tested (either actually or through simulation) and documented as part of the capability test.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(6)(i); NIST SP: 800-84, 800-115; OMB Memo: M-16-04; IRS1075; CJIS 5.6	CP-4, IR-8

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization defines incident response tests;
(ii) The organization defines in the security plan, explicitly or by reference, the frequency of incident response tests and the frequency is at least every 365 days;
(iii) The organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency;
(iv) The organization documents the results of incident response tests/exercises; and
(v) The organization determines the effectiveness of the incident response capability.

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident response testing; incident response test records; system security plan; incident response plan; and other relevant documents or records.
Examine: Records verify that organization tests the incident response capability at least as often as required by control.
Examine: Records verify that organization uses NIST SP 800-61-compliant reviews, analyses, and simulations to perform incident response capability tests.
Interview: Organizational personnel with responsibility for incident response.

IR-03(01): AUTOMATED TESTING

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS	
The organization: a. Tests incident response capability using: 1. Checklists; 2. Walk-through, discussion-based, or tabletop exercises; 3. Comprehensive, functional exercises executed in a simulated operational environment; and 4. Automated mechanisms, as applicable. b. Documents results for assessment and potential process improvement.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities, for example: (i) by providing more complete coverage of incident response issues; (ii) by selecting more realistic test scenarios and test environments; and (iii) by stressing the response capability.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-61rev2, 800-84	AT-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Tests incident response capability using checklists, tabletop exercises, comprehensive functional exercises executed in a simulated operational environment, and automated mechanisms, as applicable; (ii) Documents results for assessment and potential process improvement; and (iii) Meets all of the requirements in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident response testing; incident response test records; system security plan; incident response plan; incident response checklists; and other relevant documents or records. Examine: Records verify that organization uses checklists in incident response capability tests. Examine: Records verify that organization uses walk-through, discussion-based, or tabletop exercises in incident response capability tests. Examine: Records verify that organization uses comprehensive, functional exercises in incident response capability tests. Examine: Records verify that organization uses automated mechanisms (if applicable) in incident response capability tests. Examine: Records verify that organization uses NIST SP 800-61-compliant reviews, analyses, and simulations to perform incident response capability tests. Interview: Organizational personnel with responsibility for incident response.	

IR-03(02): COORDINATION WITH RELATED PLANS

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization coordinates incident response testing with organizational elements responsible for related plans.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization coordinates incident response testing with organizational elements responsible for related plans.	

ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; procedures addressing incident response testing; incident response test records; system security plan; incident response plan; and other relevant documents or records. Examine: Records verify that organization coordinates tests of the incident response capability with other related organizational entities. Interview: Organizational personnel with responsibility for incident response.

IR-04: INCIDENT HANDLING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Implements an incident handling capability (i.e., system incident response plan) using the current HHS Incident Response Framework and Security Incident Response Plan. b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises and implements the resulting changes accordingly.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.5 - The organization follows CMS guidance for Incident Handling, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/ **CMS-ARS:** Std.1 - Document relevant information related to a security incident according to the current HHS Security Incident Response Plan. Std.2 - Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence (i.e., Federal Rules of Evidence). Std.3 - Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure, including isolation or system disconnect. Std.4 - Incident response activities, to include forensic malware analysis, is coordinated with the ISO and HHS Information Security. Each organization's security operations center: (a) Is responsible for actions to reduce the risk that an information security and/or privacy incident will occur and to respond appropriately to each incident or breach; and (b) Maintains primary responsibility for incident detection, including internal security monitoring and analysis of network traffic and logs. Std.5 - Contact information for individuals with incident handling responsibilities must be maintained within CFACTS. (a) Changes must be documented within CFACTS within three (3) days of the change. Std.6 **-** Implements an incident handling capability (i.e., system incident response plan) using the current RMH, Volume II, Procedure 7.2, Incident Handling; Cloud: Std.6 - For cloud service providers, the organization ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.	
SUPPLEMENTAL GUIDANCE	
Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources, including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities, including, for example, mission/Information Owner(s)/Custodian(s)s, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). PII:	

A strategic, well-thought-out security incident response program will integrate with privacy incident and breach response where appropriate, with the two processes being mutually supportive.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Executive Order: 13587; FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HHS: Policy for Monitoring Employee Use of HHS IT Resources; HIPAA: 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61; OMB Memo: M-16-04; IRS1075; CJIS 5.6	AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7, SE-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization implements an incident handling capability for security incidents that includes:
- Preparation;
- Detection and analysis;
- Containment;
- Eradication; and
- Recovery.
(ii) The organization coordinates incident handling activities with contingency planning activities;
(iii) The organization incorporates lessons learned from ongoing incident handling activities into:
- Incident response procedures;
- Training; and
- Testing/exercises.
(iv) The organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly; and
(v) The organization meets all the requirements specified in the applicable Implementation Standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; incident response plan; and other relevant documents or records.
Examine: CFACTS to ensure incident handling contact information is being maintained.
Interview: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities.
Test: Incident handling capability for the organization.

IR-04(01): AUTOMATED INCIDENT HANDLING PROCESSES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs automated mechanisms to support the incident handling process.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Automated mechanisms support the exchange of incident handling information with HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, Federal requirements;
(b) Incident handling information sources include systems, appliances, devices, services, and applications (including databases).
(c) Incident handling information sources that do not support the exchange of information with HHS Information Security must be documented in the applicable risk assessment and security plan; and
(d) HHS Information Security directed incident handling information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by HHS, raw audit records must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

REFERENCES	**RELATED CONTROLS**

Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization:
(i) Employs automated mechanisms to support the incident handling process; and
(ii) Meets all the requirements specified in the applicable Implementation Standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; and other relevant documents or records.
Examine: Information system provides an automated support for incident handling.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement the incident handling process.

IR-04(03): CONTINUITY OF OPERATIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS

The organization identifies incidents and responses to classes of incident to ensure continuation of organizational missions and business functions. Classes of incident are based on attack vector (e.g., attack via external media, the web, improper system use, loss of equipment) and serve to further define specific handling procedures.

CMS-ARS:
The organization identifies emergencies, vandalism, security incidents, or natural disasters and reasonable and appropriate policies and procedures consistent with federal laws and regulations and organizational requirements to ensure continuation of organizational missions and business functions.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Incident response policies/procedures and business continuity processes should be aligned. Computer security incidents undermine the business resilience of an organization. Business continuity planners should be made aware of incidents and their impacts so they can adjust business impact, risk, and continuity of operations assessments and plans.
Std.2 - Organizations should create written guidelines for prioritizing incidents.

SUPPLEMENTAL GUIDANCE

HIPAA requires administrative, physical and technical safeguards for the protection and access of PHI during an emergency or other occurrence.

Organizations establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain PHI including procedures to enable continuation of critical business processes for the protection of PHI and for obtaining necessary PHI during an emergency. Additionally, HIPAA requires organizations to conduct a risk analysis to determine whether and to what extent they establish procedures that allow facility access in support of restoration of lost data under the disaster recovery plan in the event of an emergency.

REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-16-04; 45 C.F.R. §164.308(a)(7)(i); 45 C.F.R. §164.308(a)(7)(ii)(B); 45 C.F.R. §164.308(a)(7)(ii)(C); 45 C.F.R. §164.312(a)(2)(ii); 45 C.F.R. §164.310(a)(2)(i); CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization employs automated mechanisms to support the incident handling process.

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident handling; incident response plan; continuity of operations documentation; and other relevant documents or records.
Interview: Organizational personnel with incident handling responsibilities.

IR-04(04): INFORMATION CORRELATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS	
The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Sometimes the nature of a threat event, for example, a hostile cyber-attack, is such that it can only be observed by bringing together information from different sources, including various reports and reporting procedures established by organizations.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-61r2; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization employs automated mechanisms to support the incident handling process.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; and other relevant documents or records. Examine: Information system provides automated support for incident information correlation. Examine: Records demonstrating that the organization collects and correlates incident data from separate information systems to provide an organization-wide view of incident awareness and response. Interview: Organizational personnel with incident handling responsibilities.	

IR-04(06): INSIDER THREATS - SPECIFIC CAPABILITIES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization defines and implements the incident handling capability for insider threats.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: IS2P2; HHS: Policy for Monitoring Employee Use of HHS IT Resources	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Implements incident handling capability for insider threats; and (ii) Meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident handling; incident response plan; and other relevant documents or records. Interview: Organizational personnel with incident handling responsibilities. Test: Insider threat incident handling capability for the organization.	

IR-04(07): INSIDER THREATS - INTRA-ORGANIZATION COORDINATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization coordinates incident handling capability for insider threats across the CMS enterprise.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Insider threat coordination must be in accordance with the insider threat capability defined by CMS.	
SUPPLEMENTAL GUIDANCE	
This includes coordination with the CMS Counterintelligence & Insider Threat Program Office. Interview: Organizational personnel with incident handling responsibilities;	

Test: Insider threat incident handling capability for the organization.	
REFERENCES	**RELATED CONTROLS**
Federal: IS2P2; HHS: Policy for Monitoring Employee Use of HHS IT Resources	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Defines components or elements of the organization with whom the incident handling capability for insider threats is to be coordinated; (ii) Coordinates incident handling capability for insider threats across organization-defined components or elements of the organization; and (iii) Meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Assessment Methods and Objects: Examine: Incident response policy; procedures addressing incident handling; incident response plan; other relevant documents or records. Interview: Organizational personnel with incident handling responsibilities; Test: Insider threat incident handling capability for the organization.	

IR-05: INCIDENT MONITORING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The HHS organization tracks and documents information system security incidents. **CMS-ARS:** The organization tracks and documents all physical, information security, and privacy incidents. **IRS:** The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The organization forwards information system security and privacy incident and breach information: - In accordance with reporting requirements defined under the current HHS Incident Response Framework or applicable incident response plans, whichever is sooner; and - Provides incident and breach information in format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements. **CJIS:** Std.2 - The ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.	
SUPPLEMENTAL GUIDANCE	
Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time. PII: Tracking and documenting security and privacy incidents enables the organization to respond more effectively and evaluate both individual incidents and trends across incidents over time.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS Policy **State:** DIS Security Control Standards Catalog	AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7, SE-02

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D); 45 C.F.R. §164.308(a)(6)(ii); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization:
(i) Tracks and documents all physical, information system security, and privacy incidents;
(ii) Meets all the requirements specified in the applicable Implementation Standard(s); and
(iii) Has an organization-wide Security Information and Event Management (SIEM) capability. Additionally, SIEM information must be forwarded to HHS Information Security in accordance with HHS, and if applicable, federal requirements.

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; and other relevant documents or records.
Examine: Information systems forward security and privacy event logs to a centralized management service for aggregation, analysis, and monitoring.
Interview: Organizational personnel with incident monitoring responsibilities.
Test: Incident monitoring capability for the organization.

IR-05(01): AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers or other electronic databases of incidents.

REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-137	AU-7, IR-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

ASSESSMENT METHODS AND OBJECTS

Examine: Incident response policy; procedures addressing incident tracking and analysis; automated mechanisms supporting incident tracking and analysis; and other relevant documents or records.
Examine: Information system provides automated support for incident tracking and analysis.
Interview: Organizational personnel with incident handling responsibilities.
Test: Automated mechanisms that support and/or implement the incident tracking and analysis.

IR-06: INCIDENT REPORTING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Requires personnel to report actual or suspected security and privacy incidents to the organizational incident response capability within the timeframe established in the current HHS Security Incident Response Framework; and
b. Reports security incident information to designated personnel in the HHS Security Incident Management Plan.

CMS-MARS-E:
a. Requires personnel to report actual or suspected security and privacy incidents to the organizational incident response capability within the timeframe established in the current HHS Security Incident Response Framework and ACA incident handling process available at:
https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

IRS:
The agency must:
c. Contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than 24 hours after identification of a possible issue involving FTI. Refer to Section 10.0, Reporting Improper Inspections or Disclosures, for more information on incident reporting requirements required by the Office of Safeguards.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Security incidents shall be promptly reported to immediate supervisors and the Chief Information Security Officer. Security incidents that require timely reporting to the Department of Information Resources (DIR) include those events that are assessed to:
1. Propagate to other state systems;
2. Result in criminal violations that shall be reported to law enforcement; or
3. Involve the unauthorized disclosure or modification of confidential information, e.g., sensitive personal information as defined in §521.002(a)(2), Business and Commerce Code, and other applicable laws that may require public notification.
Std.2 - If the security incident is assessed to involve suspected criminal activity (e.g., violations of Chapters 33, Penal Code (Computer Crimes) or Chapter 33A, Penal Code (Telecommunications Crimes)), the security incident shall be investigated, reported, and documented in a manner that restores operation promptly while meeting the legal requirements for handling of evidence.
Std.3 - Depending on the criticality of the incident, it will not always be feasible to gather all the information prior to reporting. In such cases, incident response teams should continue to report information to DIR as it is collected. DIR shall instruct state organizations as to the manner in which they shall report such information to DIR. Supporting vendors or other third parties that report security incident information to a state organization shall submit such reports to the state organization in the form and manner specified by the department, unless otherwise directed by the state organization.
Std.4 - Summary reports of security-related events shall be sent to the Texas Department of Information Resources (DIR) on a monthly basis no later than nine (9) calendar days after the end of the month. The agency shall submit summary security incident reports in the form and manner specified by DIR. Supporting vendors or other third parties that report security incident information to an agency shall submit such reports to the agency in the form and manner specified by the department, unless otherwise directed by the agency.
Std.5 - In the event of a breach or suspected breach of system security or an unauthorized exposure of that information:
a. comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and
b. not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify:
1. DIR, including the State CISO and the state cybersecurity coordinator; or
2. if the breach, suspected breach, or unauthorized exposure involves election data, the Texas Secretary of State.

CMS-ARS:
(Cloud):
Std.5 - For cloud service providers, this Standard replaces the above Control. The organization requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST SP 800-61 (as amended).

SUPPLEMENTAL GUIDANCE

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling.
For more information see the see the HHS Incident Response Framework.

PII: Incidents involving personally identifiable information (PII) must be reported to the appropriate incident response center, e.g., US-CERT or Intelligence Community Security Coordination Center.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy; IS-Incident Response Framework; IS-Incident Management Plan **State:** TAC 202.23(b); TGC 2054.1125; DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(6)(ii), 45 C.F.R. §164.314(a)(2)(i); 45 C.F.R. §164.314(a)(2)(i)(C); 45 C.F.R. Part 164 Subpart D; NIST SP: 800-61; OMB Memo: M-07-16, M-16-04; Web: us-cert.gov; IRS1075; CJIS 5.6	IR-4, IR-5, IR-8, SE-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization requires personnel to report suspected security incidents to the organizational incident response capability within the timeframe established in the current HHS Incident Response Framework (ii) The organization reports security incident information to designated authorities; and (iii) The organization meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; system security plan; incident response plan; and other relevant documents or records. Examine: Information systems provide the functionality to report actual or suspected security incidents to the organizational incident response capability. Examine: Organization facilitates required oversight of incident reporting by CMS (including coordination and cooperation with HHS Information Security). Interview: Organizational personnel with incident reporting responsibilities. Test: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of incident information.	

IR-06(01): AUTOMATED REPORTING

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to assist in the reporting of security incidents.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-61; Web: us-cert.gov; CJIS 5.6	IR-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; and other relevant documents or records. Examine: Information system provides automated support for incident reporting. Interview: Organizational personnel with incident handling responsibilities. Test: Automated mechanisms that support and/or implement incident reporting.	

IR-06(02): VULNERABILITIES RELATED TO INCIDENTS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization reports information system vulnerabilities associated with reported security incidents in accordance with IR-6.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization defines personnel or roles to whom information system vulnerabilities associated with reported security incidents are to be reported; and reports information system vulnerabilities associated with reported security incidents to organization-defined personnel or roles.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident reporting; incident response plan; security plan; security incident reports and associated information system vulnerabilities; other relevant documents or records. Interview: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities; system/network administrators; personnel to whom vulnerabilities associated with security incidents are to be reported. Test: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing reporting of vulnerabilities associated with security incidents.	

IR-07: INCIDENT RESPONSE ASSISTANCE

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. The HHS CISO is available for assistance at mailto:InfoSecurity@hhsc.state.tx.us. Security incident response resources and privacy incident and breach response resources must know which resources are available, and how and when to coordinate. PII: Incident response assistance for incidents involving PII may include use of the forensic, technical, policy, and legal expertise of the organization's Information Assurance Officers/Managers, Privacy Officers, Legal Counsel, external or internal IT help desks, and the organization's Computer Emergency Response Team (CERT), in investigating and remediating incidents.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(ii); OMB Memo: M-16-04; 45 C.F.R. §164.308(a)(6)(i); IRS1075; CJIS 5.6	AT-2, IR-4, IR-6, IR-8, SA-9, SE-02

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if: (i) The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; (ii) The incident response support resource is an integral part of the organization's incident response capability; and (iii) The organization meets all the requirements specified in the applicable Implementation Standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; other relevant documents or records. Interview: Organizational personnel with incident response assistance and support responsibilities. Interview: Organizational personnel with incident management responsibilities.

IR-07(01): AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to increase the availability of incident response-related information and support.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability or, conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.
ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; procedures addressing incident response-related information and support; automated mechanisms supporting incident response-related information and support and other relevant documents or records. Examine: Information system provides automated support for pushing or pulling incident response-related information on demand by authorized users. Interview: Organizational personnel with incident handling responsibilities. Test: Automated mechanisms that support and/or implement incident response-related information push/pull.

IR-07(02): COORDINATION WITH EXTERNAL PROVIDERS

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization: a. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and b. Identifies organizational incident response team members to the external providers.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

External providers of information system protection capability include, for example, the Computer Network Defense program within the DoD. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.	
REFERENCES	**RELATED CONTROLS**
Federal: Cybersecurity Enhancement Act of 2014; FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization coordinates with external providers to increase the availability of incident response-related information and support.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident coordination with external providers of protection capabilities; automated mechanisms supporting incident coordination with external providers of protection capabilities; list of external providers of protection capabilities; and other relevant documents or records. Examine: Organization coordinates with external providers of protection capabilities when incidents occur, during incident response testing, and during normal operations. Interview: Organizational personnel with incident handling responsibilities.	

IR-08: INCIDENT RESPONSE PLAN

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by designated officials within HHS; b. Distributes copies of the incident response plan to incident response personnel and HHS organizational elements; c. Reviews the incident response plan within every three hundred sixty-five (365) days; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to incident response personnel and relevant HHS stakeholders; f. Protects the incident response plan from unauthorized disclosure and modification.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The organization defines a list of incident response personnel (identified by name and/or by role), designated CMS personnel and organizational elements for the following: a. Distribution of the response plan b. Communication of any changes Std.2 - The organization follows CMS guidance for Incident Handling, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. PHI:	

In developing an incident response plan, ensure it incorporates guidance from the privacy office for the handling of incidents involving PHI. PII: In developing an incident response plan, ensure it incorporates guidance from the Privacy Office for the handling of incidents involving personally identifiable information (PII).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; NIST SP: 800-61; 45 C.F.R. §164.308(a)(6)C.F.R.; IRS1075; CJIS 5.6	MP-2, MP-4, MP-5, SE-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization develops an incident response plan that: (i) Provides the organization with a roadmap for implementing its incident response capability; (ii) Describes the structure and organization of the incident response capability; (iii) Provides a high-level approach for how the incident response capability fits into the overall organization; (iv) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; (v) Defines reportable incidents; (vi) Provides metrics for measuring the incident response capability within the organization; (vii) Defines the resources and management support needed to effectively maintain and mature an incident response capability; (viii) Is reviewed and approved by the applicable Incident Response Team Leader; and (ix) Is routinely followed in response to incidents.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident response assistance; incident response plan; and other relevant documents or records. Interview: Organizational personnel with incident response planning responsibilities. Test: Organizational incident response plan and related organizational processes. NOTE: The organization incident response capability must be able to demonstrate knowledge of the incident response processes and procedures and evidence showing the plan is followed routinely while responding to incidents.	

IR-09: INFORMATION SPILLAGE RESPONSE

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting incident response personnel (as defined in the SSP and the incident response plan [See IR-6]) of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing required response actions as in the system incident response plan.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The organization responds to information spills by requiring personnel to report suspected incidents to the organizational incident response capability within the timeframe established in the current Administering Entity (AE) organization Incident Handling Procedure and ACA incident handling reporting process available at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.
ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; information spillage policy; procedures addressing incident reporting; procedures addressing information spillage response; list of information (or information types) that could be included in an information spillage; and other relevant documents or records. Examine: Organization follows appropriate procedures when responding to information spillage. Interview: Organizational personnel with incident handling responsibilities.

IR-09(01): RESPONSIBLE PERSONNEL

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization assigns responsibility for responding to information spills to defined personnel or roles.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization: (i) Defines personnel with responsibility for responding to information spills; (ii) Assigns organization-defined personnel with responsibility for responding to information spills; and (iii) Meets all the requirements specified in the applicable Implementation Standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; procedures addressing information spillage; incident response plan; list of personnel responsible for responding to information spillage; and other relevant documents or records. Interview: Organizational personnel with incident response responsibilities.

IR-09(02): TRAINING

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization provides information spillage response training no less often than annually.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.
ASSESSMENT METHODS AND OBJECTS
Examine: Incident response policy; information spillage policy; procedures addressing incident reporting; procedures addressing information spillage response; list of information (or information types) that could be included in an information spillage; and other relevant documents or records. Examine: Information system includes capability to track participation in information spillage training activities. Interview: Organizational personnel with information spillage training and operational responsibilities.

IR-09(03): POST-SPILL OPERATIONS

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization implements processes procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; information spillage policy; procedures addressing incident reporting; procedures addressing information spillage response; list of information (or information types) that could be included in an information spillage; and other relevant documents or records. Examine: Organization follows appropriate procedures when responding to information spillage. Interview: Organizational personnel with incident handling responsibilities.	

IR-09(04): EXPOSURE TO UNAUTHORIZED PERSONNEL

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs CMS rules of behavior and information system defined security safeguards and privacy to address the risk of personnel exposed to information not within assigned access authorizations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; information spillage policy; procedures addressing incident reporting; procedures addressing information spillage response; list of information (or information types) that could be included in an information spillage; and other relevant documents or records. Examine: Appropriate personnel follow all mandated policies and guidance when assessing the risks posed by or to personnel exposed to information not within their assigned access authorizations.	

IR-10: INTEGRATED INFORMATION SECURITY ANALYSIS TEAM

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

The integrated information security analysis team will support the organization's personally identifiable information (PII) incident response team (as specified in OMB M-07-16) in all aspects of response to a security incident involving PII.	
REFERENCES	**RELATED CONTROLS**
Federal: Cybersecurity Enhancement Act of 2014; OMB Memo: M-07-16, M-16-04	SE-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Establishes an integrated team of forensic/malicious code analyst, tool developers, and real-time operations personnel; and (ii) Meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Incident response policy; procedures addressing incident response planning and security analysis team integration; incident response plan; and other relevant documents or records. Examine: Organization facilitates required oversight and coordination information security and privacy incident response teams by CMS (including coordination and cooperation with HHS Information Security). Interview: Organizational personnel with incident response and information security analysis responsibilities; organizational personnel with information security responsibilities; organizational personnel participating on integrated security analysis teams.	

(MA) MAINTENANCE

The HHS organization requires that (i) periodic and timely maintenance on HHS information systems occur; and (ii) effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance are in place.

MA-01: SYSTEM MAINTENANCE POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls. b. Reviews and updates (as necessary) the current: 1. System maintenance policy within every three (3) years; and 2. System maintenance procedures within every three hundred sixty five (365) days. **CMS-MARS-E:** b.1. System maintenance policy within every three hundred sixty five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - PII: System maintenance policy and procedures must ensure that contractors having access to records (i.e., files or data) maintained in a system of records are contractually bound to be covered by the Privacy Act.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PHI:	

Procedures to facilitate the implementation of the system maintenance policy should include access control validation and accountability procedures. PII: Privacy considerations should be included in system maintenance policy and procedures especially when the system contains information subject to the Privacy Act and/or HIPAA.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(d)(2)(iii); NIST SP: 800-12, 800-100; IRS1075; CJIS 5.6	PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators.	

MA-02: CONTROLLED MAINTENANCE

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on-site or removed to another location; c. Requires that the applicable Information Owner(s)/Custodian(s) (or an official designated in the applicable security plan) explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes the following in HHS organizational maintenance records: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) Description of the maintenance performed; and, (e) List of equipment removed or replaced (including identification numbers, if applicable).	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - In facilities where Personal Identifiable Information (PII) is stored or accessed, document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).	
SUPPLEMENTAL GUIDANCE	
This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example:	

(i) Date and time of maintenance; (ii) Name of individuals or group performing the maintenance; (iii) Name of escort, if necessary; (iv) Description of the maintenance performed; and (v) Information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. HIPAA: HIPAA requires organizations to apply reasonable and appropriate safeguards for the protection of PHI, including implementing policies and procedures to document repairs and modifications to the facility which are related to security. Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(d)(2)(iii); IRS1075; CJIS 5.6	CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators. Test: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms implementing sanitization of information system components.	

MA-02(02): AUTOMATED MAINTENANCE ACTIVITIES

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and b. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	CA-7, MA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators. Test: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms implementing sanitization of information system components.

MA-03: MAINTENANCE TOOLS

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization approves, controls, and monitors information system maintenance tools.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; NIST SP: 800-88; IRS1075	MA-2, MA-5, MP-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.	

MA-03(01): INSPECT TOOLS

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-88	SI-7
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-03(02): INSPECT MEDIA

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-88; CJIS 5.6	SI-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.	

MA-03(03): PREVENT UNAUTHORIZED REMOVAL

Priority: P3	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E, CJIS
CONTROL REQUIREMENTS	
The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: a. Verifying that there is no organizational information contained on the equipment; b. Sanitizing or destroying the equipment; c. Retaining the equipment within the facility; or d. Obtaining an exemption, in writing, from the HHS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - For cloud service providers, this Standard replaces the above Enhancement. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no sensitive information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.	
SUPPLEMENTAL GUIDANCE	
Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-88; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; and other relevant documents or records.

MA-04: NONLOCAL MAINTENANCE

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with HHS organizational policy and documented in the system security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. Std.2 - Media used during remote maintenance must be sanitized in accordance with NIST SP 800-88, as amended.	
SUPPLEMENTAL GUIDANCE	
Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2, 197, 201; FISCAM: AS-1, SM-7; NIST SP: 800-63, 800-88; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R. §164.312(d); 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(ii); IRS1075; CJIS 5.6	AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities	

MA-04(01): AUDITING AND REVIEW

Priority: P2

Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization: a. Audits nonlocal maintenance and diagnostic sessions using available audit events; and b. Reviews the records of the maintenance and diagnostic sessions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	AU-2, AU-6, AU-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan; information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities Examine: Audit records for nonlocal maintenance and diagnostic sessions. Examine: Documentation verifying that the organization performs reviews of audit records for nonlocal maintenance and diagnostic sessions.	

MA-04(02): DOCUMENT NONLOCAL MAINTENANCE

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan (SSP); information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities Examine: Documentation in the SSP of the policies and procedures covering maintenance and diagnostic connections.	

MA-04(03): COMPARABLE SECURITY / SANITIZATION

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MAR-E
CONTROL REQUIREMENTS	
The organization:	

a. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or b. Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced.

REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-63, 800-88	MA-3, SA-12, SI-3, SI-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system maintenance policy; procedures addressing nonlocal maintenance for the information system; system security plan (SSP); information system design documentation; information system configuration settings and associated documentation; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities Examine: Documentation in the SSP of the policies and procedures covering maintenance and diagnostic connections.

MA-04(06): CRYPTOGRAPHIC PROTECTION

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Encrypting the communications channel when maintenance is performed remotely protects user credentials, sensitive information such as personally identifiable information (PII), and other data as it travels “across the wire.”	

REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 140-2; NIST SP: 800-63, 800-88; CJIS 5.6	SC-8, SC-13

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.
ASSESSMENT METHODS AND OBJECTS
Examine: Information system maintenance policy; procedures addressing non-local information system maintenance; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators. Test: Cryptographic mechanisms protecting nonlocal maintenance and diagnostic communications.

MA-04(07): REMOTE DISCONNECT VERIFICATION

Priority:

Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing non-local information system maintenance; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators. Test: Automated mechanisms implementing remote disconnect verifications of terminated nonlocal maintenance and diagnostic sessions.	

MA-05: MAINTENANCE PERSONNEL

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The state organization allows only authorized personnel to perform maintenance on the information system.	
SUPPLEMENTAL GUIDANCE	
This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems, while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, system integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. PHI: Under HIPAA, this is an addressable control. PII: If maintenance personnel are contractors, then the organizations personnel responsible for contracting (such as the contracting officer [KO or CO], contracting officer's representative [COR], or contracting officer's technical	

representative [COTR]) or the program manager (PM) must ensure that contractors having access to records (i.e., files or data) from a system of records are contractually bound to be covered by the Privacy Act.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(a)(2)(iv); 45 C.F.R. §164.310(d)(2)(iii); IRS1075; CJIS 5.6	AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3, SA-4, AR-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing maintenance personnel authorization; maintenance personnel rules of behavior; system security plan; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities Examine: Procedures governing maintenance personnel authorization, escort/supervision, and work execution. Examine: Documentation verifying that the organization follows documented maintenance personnel policy and procedures	

MA-05(01): INDIVIDUALS WITHOUT APPROPRIATE ACCESS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured. b. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	MP-6, PL-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing maintenance personnel that lack appropriate security clearances or citizenship; maintenance personnel rules of behavior; system security plan; maintenance records; and other relevant documents or records.	

Interview: Organizational personnel with information system maintenance responsibilities Examine: Procedures governing maintenance personnel authorization, escort/supervision, and work execution. Examine: Documentation verifying that the organization follows documented maintenance personnel policy and procedures, including sanitization of volatile storage components and removal of non-volatile storage components before uncleared or non-US-citizen maintenance personnel initiate maintenance or diagnostic activities.

MA-05(04): FOREIGN NATIONALS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization ensures that: (a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and (b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	PS-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization ensures that: cleared foreign nationals (i.e., foreign nationals with appropriate security clearances) are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are: jointly owned and operated by the United States and foreign allied governments; or owned and operated solely by foreign allied governments; and approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing maintenance personnel; information system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; memorandum of agreement; maintenance records; access control records; access credentials; access authorizations; other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities, organizational personnel with personnel security responsibilities; organizational personnel managing memoranda of agreements; organizational personnel with information security responsibilities. Test: Organizational processes for managing foreign national maintenance personnel.	

MA-06: TIMELY MAINTENANCE

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable RTO specified in the contingency plan.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - For cloud service providers, this Standard replaces the above Control. The organization defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the JAB. Std.2 - For cloud service providers, the organization defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.	

SUPPLEMENTAL GUIDANCE	
Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iv)	CM-8, CP-2, CP-7, SA-14, SA-15
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system maintenance policy; procedures addressing maintenance for the information system; information system contingency plan; system security plan; vendor maintenance agreements; maintenance records; and other relevant documents or records. Interview: Organizational personnel with information system maintenance responsibilities; system/network administrators. Examine: Documentation verifying that maintenance support and/or spare parts are obtained within the applicable RTO specified in the contingency plan.	

(MP) MEDIA PROTECTION

The HHS organization (i) requires the protection of digital and non-digital information system media (ii) limits access to information on information system media to authorized users; and (iii) sanitizes or destroys information system media before disposal or release for reuse.

MP-01: MEDIA PROTECTION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls. b. Reviews and updates (as necessary) the current: 1. Media protection policy within every three (3) years; and 2. Media protection procedures within every three hundred and sixty five (365) days. **CMS-MARS-E:** b.1. Media protection policy within three hundred and sixty five (365) days; and.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Applicable personnel (item a) include employees and contractors with potential access to protected health information (PHI). Std.2 - Applicable personnel (item a) include employees and contractors with potential access to personally identifiable information (PII). **CMS-MARS-E:** Std.1 - Semi-annual inventories of removable media containing Personally Identifiable Information (PII) are conducted. The organization accounts for any missing removal media containing PII by documenting the search efforts and notifying the media initiator of the loss.	

Std.1 - The media protection policy and procedures specify that the term "information system media" includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm).
SUPPLEMENTAL GUIDANCE
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST Special Publications 800-12, 800-100**;** IRS1075; CJIS 5.6	PM-9

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; and other relevant documents or records. Interview: Organizational personnel with information system media protection responsibilities.

MP-02: MEDIA ACCESS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, high	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization restricts access to HHS confidential, and agency sensitive media to authorized individuals defined in the applicable security plan. **CMS-MARS-E:** The organization restricts access to sensitive information, such as Personally Identifiable Information (PII), residing on digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas. **CMS-ARS:** The organization restricts access to sensitive digital and non-digital media pursuant to Appendix I of HHS Information System Security and Privacy Policy (IS2P) and in compliance with the latest revision of NIST SP 800-88, Guidelines for Media Sanitization, to defined personnel or roles (defined in the applicable security plan) by disabling: - CD/DVD writers and allowing access to defined personnel or roles; and - USB ports and allowing access to defined personnel or roles.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Sensitive digital and non-digital media includes media containing protected health information (PHI). Std.2 - Sensitive digital and non-digital media includes media containing personally identifiable information (PII). Std.3 - Defined personnel or roles must be authorized individuals with a valid need to know.	
SUPPLEMENTAL GUIDANCE	
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals	

seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team.

PII:
Restricting access to digital and non-digital media, including mobile devices with storage capabilities, protects sensitive information, such as PII, from unauthorized use and disclosure. A risk assessment should be conducted to determine what sensitive information if any, can be stored on certain media types and who is authorized to do so.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 164.312(c)(1); 45 C.F.R. §164.310(c); 45 C.F.R. §164.310(d)(1); NIST SP: 800-88, 800-111; IRS1075; CJIS 5.6	AC-2, AC-3, IA-2, MP-4, PE-2, PE-3, PL-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; and other relevant documents or records.
Interview: Organizational personnel with information system media protection responsibilities.

MP-03: MEDIA MARKING

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts specific types of media or hardware components, as specified, in writing, by the HHS CIO or his/her designated representative, from marking as long as the media remain within a secure environment.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Stored data must have, at a minimum, the following data clearly identifiable by labels and/or other coding systems:
a. System Name
b. Creation Date
c. Sensitivity Classification (based on applicable record retention regulations)
d. HHS Contact Information

IRS:
Std.2 - The agency must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating “Federal Tax Information”. Notice 129-A and Notice 129-B IRS provided labels can be used for this purpose.

SUPPLEMENTAL GUIDANCE

The term security marking refers to the application/use of human-readable security attributes. The term security labeling refers to the application/use of security attributes with regard to internal data structures within information systems (see AC-16). Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Security marking is generally not required for media containing information determined by organizations to be in the public domain or to be publicly releasable. However, some organizations may require markings for public

information indicating that the information is publicly releasable. Marking of information system media reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. PII: Media containing personally identifiable information (PII), or the container for the media if labeling the media is not practicable, must be marked appropriately. Reflects applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FIPS Publication 199; IRS1075; CJIS 5.6	AC-16, PL-2, RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; system security plan; removable storage media and information system output; and other relevant documents or records. Interview: Organizational personnel with information system media protection and marking responsibilities.	

MP-04: MEDIA STORAGE

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Physically controls and securely stores confidential and agency sensitive data within controlled areas; and b. Protects information system media (which includes both digital and non-digital media) until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Media used in the provision of backup storage must be protected in accordance with the highest level of sensitivity of the information being stored. Std.2 - Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash/thumb drives, diskettes, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm). Std.3 – For confidential data, encrypt digital media via a FIPS 140-2 compliant encryption module. Std.4 - If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information. **CMS-ARS, CMS-MARS-E, IRS, CJIS:** Std.3 – For confidential data, encrypt digital media via a FIPS 140-2 validated encryption module. **SPI:** Std.5 - The applicant/bidder prohibits the access, creation, disclosure, reception, transmission, maintenance, and storage of HHS Confidential Information with a subcontractor (e.g. cloud services, social media, etc.) unless HHS has approved the subcontractor agreement which must include compliance and liability clauses with the same requirements as the applicant/bidder. **CMS-MARS-E:** Std.5 - For non-digital media, provides secure storage in locked cabinets or safes. **IRS:** Std.5- See Section 4.0, Secure Storage—IRC 6103(p)(4)(B), on additional secure storage requirements.	
SUPPLEMENTAL GUIDANCE	
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video	

disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas or spaces for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection.

PII:
Controlling the storage of media containing sensitive information such as PII protects the media from theft and promotes accountability.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.310(c), 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(iv); NIST SP: 800-56, 800-57, 800-88, 800-111; IRS1075; CJIS 5.6	CP-6, CP-9, MP-2, MP-7, PE-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; information system media; and other relevant documents or records.
Interview: Organizational personnel with information system media protection and storage responsibilities

MP-05: MEDIA TRANSPORT

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Protects and controls digital media during transport outside of controlled areas using encryption and for non-digital media tamper-evident packaging and
1. if hand carried, using a securable container (e.g., locked briefcase) via authorized personnel, or
2. if shipped, trackable with receipt by commercial carrier.
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of HHS information system media; and
d. Restricts the activities associated with transport of HHS information system media to authorized personnel.

IRS:
b. Document activities associated with the transport of information system media— the agency must use transmittals or an equivalent tracking method to ensure FTI reaches its intended destination
See Section 4.4, FTI in Transit, for more information on transmittals and media transport requirements.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - Service providers protect and control magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas using for digital media, encryption using a FIPS 140-2 validated module.
Std.2 - Service providers define security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.

CMS-MARS-E:
Std.1 - Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.
Std.2 - The organization protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks, and digital video disks during transport outside of controlled areas, and encrypts digital media via a FIPS 140-2 validated encryption module.
Std.3 - The organization defines security measures to protect digital and non-digital media in transport.

IRS:
Std.1 - The information system must implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. (See MP-5(4))
Std.2 - Handling FTI must be such that the FTI does not become misplaced or available to unauthorized personnel.
Std.3 - Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards. When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures
Std.4 - All shipments of paper or electronic FTI (including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes, and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is, one envelope within another envelope. The inner envelope must be marked "confidential" with some indication that only the designated official or delegate is authorized to open it. The outermost envelope should not be labelled as FTI or provide any indication that the contents contains FTI, since that may actually increase risk to the contents. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

SUPPLEMENTAL GUIDANCE

Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers), that are transported outside of controlled areas. Controlled areas are areas or spaces for which organizations provide sufficient physical and/or procedural safeguards to meet the requirements established for protecting information and/or information systems.

Physical and technical safeguards for media are commensurate with the security category or classification of the information residing on the media. Safeguards to protect media during transport include, for example, locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Maintaining accountability of media during transport includes, for example, restricting transport activities to authorized personnel and tracking and/or obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with organizational assessments of risk to include the flexibility to define different record-keeping methods for the different types of media transport as part of an overall system of transport-related records.

PII:
Protecting and controlling media containing sensitive information, such as PII, commensurate with the sensitivity of the information contained on the media, during transport outside of controlled areas, promotes accountability and limits situations that make the media vulnerable to unauthorized use and disclosure through loss, theft, or other mishandling.

REFERENCES	RELATED CONTROLS
Federal: FIPS Publication 199; NIST Special Publication 800-60; IRS1075; CJIS 5.6	AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; and other relevant documents or records. Interview: Organizational personnel with information system media transport responsibilities.

MP-05(03): CUSTODIANS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs an identified custodian during transport of information system media outside of controlled areas.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; and other relevant documents or records. Interview: Organizational personnel with information system media transport responsibilities.	

MP-05(04): CRYPTOGRAPHIC PROTECTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement applies to both portable storage devices (e.g., USB memory sticks, compact disks, digital video disks, external/removable hard disk drives) and mobile devices with storage capability (e.g., smart phones, tablets, E-readers). PHI: Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media. PII: Encrypting portable media and mobile devices protects confidentiality and integrity of sensitive information, such as personally identifiable information (PII), stored on those devices.	
REFERENCES	**RELATED CONTROLS**

Federal: FedRAMP Rev. 4 Baseline; 45 C.F.R. §164.312(a)(2)(iv); CJIS 5.6	MP-2, CP-9

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media transport; information system media transport records; audit records; and other relevant documents or records.
Test: Cryptographic mechanisms protecting information during transportation outside controlled areas.

MP-06: MEDIA SANITIZATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Sanitizes both digital and non-digital information systems media prior to disposal, release out of organizational control, or release for reuse using sanitization techniques in accordance with applicable federal, state, and organizational standards and policies; and
b. Employs sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Employ sanitization mechanisms consistent with guidance provided in NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization and Texas Government Code §441.185.
Std.2 - Prior to the sale or transfer of data processing equipment, to other than another Texas state agency or agent of the state, state agencies shall assess whether to remove data from any associated storage device. Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the state agency shall retain a hard copy or other electronic copy of the record for the required retention period.
Std.3 - If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are provided in the "Sale or Transfer of Computers and Software" guidelines available at http://www.dir.texas.gov.
Std.4 - State agencies shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:
• date;
• description of the item(s) and serial number(s);
• inventory number(s);
• the process and sanitization tools used to remove the data or method of destruction; and
• the name and address of the organization the equipment was transferred to.
Std.5 – For cloud service providers, the hypervisor enforces sanitization of the instance (container) image file space upon release.

SPI:
Std.6 - Notwithstanding records retention requirements, the Applicant/Bidder's disposal processes for HHS Confidential Information ensures that HHS Confidential Information is destroyed so that it is unreadable or undecipherable.

CMS-ARS, CMS-MARS-E:
Low, Low Plus, Moderate, High:
Std.6 - Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures.

Moderate, High:
Std.7 - Surplus equipment is stored securely while not in use, and disposed of or sanitized in accordance with NIST 800-88 when no longer required.

CMS-MARS-E:
Std.8. Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing Personally Identified Information, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies:

(i) Date received;
(ii) Reel/cartridge control number contents;
(iii) Number of records, if available;
(iv) Movement; and
(v) If disposed of, the date and method of disposition.

IRS:
Std.6 - Agencies must review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Agencies verify that the sanitization of the media was effective prior to disposal (see Section 9.3.17.9, Information Handling and Retention (SI-12)).
Std.7 - The agency must restrict the use of information system media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) on information systems that receive, process, store, or transmit FTI using physical or automated controls.

Additional requirements for protecting FTI during media sanitization are provided in Section 9.3.10.6, Media Sanitization (MP-6); Section 9.4.7, Media Sanitization; and Exhibit 10, Data Warehouse Security Requirements.

CJIS:
Std.6 - The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals.

SUPPLEMENTAL GUIDANCE

This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information.

PII:
Properly sanitizing media that contains sensitive information, such as PII, prior to disposal or release protects the information from unauthorized use and disclosure.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** TGC 2054.130; DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.310(d)(1), 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(d)(2)(ii); NIST SP: 800-60, 800-88; Web: nsa.gov/ia/mitigation_guidance/; IRS1075; CJIS 5.6	MA-2, MA-4, RA-3, SC-4, DM-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; and other relevant documents or records. Interview: Organizational personnel with information system media sanitization responsibilities.

MP-06(01): REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The organization ensures Personally Identifiable Information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.	
SUPPLEMENTAL GUIDANCE	
Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. PII: Tracking, documenting, and verifying media sanitization and disposal actions for media that contains sensitive information, such as personally identifiable information (PII), reduces the risk of unauthorized disclosure of sensitive information and increases accountability.	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 199; NIST SP: 800-60, 800-88; 45 C.F.R. §164.310(d)(1); 45 C.F.R. §164.310(d)(2)(i); 45 C.F.R. §164.312(d)(2)(ii); CJIS 5.6	SI-12, DM-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records, audit records, and other relevant documents or records. Interview: Organizational personnel with information system medial sanitization responsibilities.	

MP-06(02): EQUIPMENT TESTING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E, CJIS
CONTROL REQUIREMENTS	
The organization tests sanitization equipment and procedures within every three hundred sixty-five (365) days to verify that the intended sanitization is being achieved.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).	
REFERENCES	**RELATED CONTROLS**

Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 199; NIST SP: 800-60, 800-88; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-06(03): NONDESTRUCTIVE TECHNIQUES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS

CONTROL REQUIREMENTS

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances:
a. Prior to initial use after purchase;
b. When obtained from an unknown source;
c. When the organization loses a positive chain of custody; and
d. When device was connected to a lower assurance network/system based on FIPS 199 security categorization.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control enhancement applies to digital media containing Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code, including code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices.

REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 199; NIST SP: 800-60, 800-88; CJIS 5.6	SI-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; and other relevant documents or records.
Interview: Organizational personnel with information system media sanitization responsibilities.

MP-06(08): REMOTE PURGING / WIPING OF INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization provides the capability to purge/wipe information from information systems, system components, and devices either remotely or as defined in the RMH Standards and Procedures.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Organizations must consider the use of this control for moderate and high personally identifiable information (PII) confidentiality impact level information on devices such as mobile devices like an iPad or other smart device. If your organization permits use of personal smart devices (for example, Bring Your Own Device

[BYOD]), the organization must evaluate methods to ensure this control is enforced or that compensating controls are in place.	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Pub: 199; NIST SP: 800-60, 800-88	DM-2, SE-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization: (i) Defines information systems, system components, or devices to purge/wipe either remotely or under specific organizational conditions; (ii) Defines conditions under which information is to be purged/wiped from organization-defined information systems, system components, or devices; and (iii) Provides the capability to purge/wipe information from organization-defined information systems, system components, or devices either: (a) Remotely; or (b) Under organization-defined conditions.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system media protection policy; procedures addressing media sanitization and disposal; information system design documentation; information system configuration settings and associated documentation; media sanitization records; audit records; and other relevant documents or records. Interview: Organizational personnel with information system media sanitization responsibilities; organizational personnel with information security responsibilities; system/network administrators. Test: Organizational processes for purging/wiping media; automated mechanisms supporting and/or implementing purge/wipe capabilities.	

MP-07: MEDIA USE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization prohibits the use of personally owned media on organizational information systems or system components using defined security safeguards in accordance with organizational policy.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - The organization restricts the use of portable storage and mobile devices on information systems and networks containing personally identifiable information (PII), without using device ownership, media sanitization and encryption controls.	
SUPPLEMENTAL GUIDANCE	
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. PII: This control applies to devices containing PII, particularly portable storage and mobile devices.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	AC-19, PL-4, SE-02

Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 199; NIST SP: 800-111; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media usage; information system audit records; and other relevant documents or records.
Examine: Information system restricts the use of portable storage devices.
Interview: Organizational personnel with information system media responsibilities; organizational personnel on use of personally owned media.
Test: Automated mechanisms implementing restrictions on the use of non-organizationally owned media.

MP-07(01): PROHIBIT USE WITHOUT OWNER

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

PII:
The ability to identify the owner of removable media that stores sensitive information, such as personally identifiable information (PII), assigns accountability and responsibility managing the media and responding to a privacy breach.

REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-111; CJIS 5.6	PL-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media usage; information system audit records; and other relevant documents or records.
Examine: Information system prohibits the use of portable storage devices when there is no identifiable device owner.
Interview: Organizational personnel with information system media responsibilities; organizational personnel on use of portable storage devices.
Test: Automated mechanisms implementing restrictions on the use of portable storage devices.

MP-08(03): CONTROLLED UNCLASSIFIED INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization downgrades information system media containing personally identifiable information (PII) prior to public release in accordance with applicable federal and organizational standards and policies.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Prior to public release of any media containing sensitive information, such as PII or protected health information (PHI), that media must be reviewed to ensure that all sensitive information has been appropriately redacted or de-identified and any file containing sensitive information on that media is appropriately sanitized so that the information is not recoverable or re-identifiable. PHI: Downgrading of media containing PHI must implement HIPAA de-identification procedures to ensure PHI may not be re-identified.

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization:
(i) Defines PII contained on information system media that require downgrading prior to public release; and
(ii) Downgrades information system media containing PII prior to public release in accordance with applicable federal and organizational standards and policies.

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; access authorization policy; procedures addressing downgrading of media containing PII; applicable federal and organizational standards and policies regarding protection of PII; media downgrading records; and other relevant documents or records.
Interview: Organizational personnel with information system media downgrading responsibilities; organizational personnel with information security responsibilities.
Test: Organizational processes for media downgrading; automated mechanisms supporting and/or implementing media downgrading.

MP-CMS-01: MEDIA RELATED RECORDS

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E

CONTROL REQUIREMENTS

Inventory and disposition records for information system media must be maintained to ensure control and accountability of sensitive information. The media related records must contain sufficient information to reconstruct the data in the event of a breach.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The media records must, at a minimum, contain:
(a) The name of media recipient;
(b) Signature of media recipient;
(c) Date/time media received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

SUPPLEMENTAL GUIDANCE

The organization employs a hash function (a reproducible method of turning inventory data into a relatively small number, which may serve as a digital "fingerprint" of the data) for electronic inventory records maintenance to validate, during investigation of a possible breach, whether the inventory information is free from tampering prior to reconstructive events.

REFERENCES	RELATED CONTROLS
Federal: OMB Memo: M-16-04	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information system media protection policy; procedures addressing media handling, ownership, and disposal; media sanitization records, audit records, and other relevant documents or records.
Interview: Organizational personnel with information system medial sanitization responsibilities

(PE) PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

The HHS organization coordinates with Texas Facilities Commission (TFC) and/or other owning facility management organizations to (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

PE-01: PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, IRS, CJIS, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. b. Reviews and updates (as necessary) the current: 1. Physical and environmental protection policy within every three (3) years; and 2. Physical and environmental protection procedures within every three hundred and sixty five (365) days. **CMS-MARS-E:** b.1. Physical and environmental protection policy every three hundred and sixty five (365) days	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PHI: Sensitivity of PHI may impact the necessary physical and environmental controls. Physical controls are important for protecting PHI against unauthorized access, use, and disclosure. Environmental controls can be critical when PHI has high availability requirements (e.g., core mission capabilities of an organization rely on consistent and frequent access to PHI).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(a)(2)(ii), 45 C.F.R. §164.310(a)(2)(iii); NIST SP: 800-12, 800-100; IRS1075; CJIS 5.6	PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Physical and environmental protection policy and procedures; and other relevant documents or records. Interview: Organizational personnel with physical and environmental protection responsibilities

PE-02: PHYSICAL ACCESS AUTHORIZATIONS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals at least every six months; d. Removes individuals from the facility access list when access is no longer required. **CMS-ARS:** c. Reviews the access list detailing authorized facility access by individuals every (90 High, 180 Moderate, 365 Low) days.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The state organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. **CMS-MARS-E:** Std.2 - Create a restricted area, security room, or locked room to control access to areas containing Personally Identifiable Information (PII). These areas will be controlled accordingly. Cloud: Std.2 - For cloud service providers, the organization reviews and approves the access list and authorization credentials at least every 365 days, removing from the access list personnel no longer requiring access.	
SUPPLEMENTAL GUIDANCE	
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. PHI: Under HIPAA, this is an addressable control. Maintaining a current list of personnel that are authorized to access facilities where sensitive information, such as personally identifiable information (PII), is located protects the information from unauthorized access.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b), (e)(10)164.310(a)(2)(iii); FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(2)(iii) OMB Circular A-130: 7.g; IRS1075; CJIS 5.6	PE-3, PE-4, PS-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; and other relevant documents or records.

PE-02(01): ACCESS BY POSITION / ROLE

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization authorizes physical access to the facility where the information system resides based on position or role. **IRS:** Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Implementing role-based access controls for physical access provides a further level of granularity in governing who can access facilities, and even certain parts of facilities, that store and process PHI. The authorization of physical access to the facility should include considerations of whether the person needs access to PHI and whether such access is permitted under the HIPAA Privacy Rule.	
REFERENCES	**RELATED CONTROLS**
Federal: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii); CJIS 5.6	AC-2, AC-3, AC-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; list of positions/roles and corresponding physical access authorizations; information system entry and exit points; other relevant documents or records. Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to information system facility; organizational personnel with information security responsibilities. Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.	

PE-02(03): RESTRICT UNESCORTED ACCESS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization restricts unescorted access to the facility where the information system resides to personnel with formal access authorizations for all information contained within the system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	PS-2, PS-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	

ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; security clearances; access authorizations; access credentials; physical access control logs or records; other relevant documents or records. Interview: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to information system facility; organizational personnel with information security responsibilities. Test: Organizational processes for physical access authorizations; automated mechanisms supporting and/or implementing physical access authorizations.

PE-03: PHYSICAL ACCESS CONTROL

Priority: P1	
Baseline(s): Low, Low Plus, Mod, SPI	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Enforces physical access authorizations at physical access points (including designated entry/exit points) to the facility where information systems reside, excluding those areas within the facility officially designated as publicly accessible, by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility containing information systems using guards and/or physical access control systems/devices; b. Maintains physical access audit logs for entry/exit points; c. Provides security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity as required; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices every year; and g. Changes combinations annually and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. **CMS-ARS:** f. Inventories defined physical access devices (defined in the applicable security plan) no less often than every (90 High, 90 Moderate, or 180 Low and Low Plus) days; and	
CONTROL IMPLEMENTATION STANDARDS	
Low, Low Plus: Std.1 - Control data center/facility access by use of door and window locks. Std.2 - Store and operate servers in physically secure environments protected from unauthorized access. Moderate, High: Std.1 - Access records, entry and exit logs, and visitor logs must be kept based on records retention or other state or federal requirements. Std.2 - Unattended portable computing devices must be physically secured by locking devices and/or locked storage. Std.3 - Control data center/facility access by use of door and window locks and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination. Std.4 - Store and operate servers in physically secure environments and grant access to explicitly authorized personnel only. Access is monitored and recorded. Std.5 - Restrict access to grounds/facilities to authorized persons only. **SPI:** Std.6 - The applicant/bidder secures physical access to computer, paper, or other systems containing HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.). **CMS-ARS, CMS-MARS-E**: PII: Std.6 - Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly.	

Std.7 - Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access afterhours.
SUPPLEMENTAL GUIDANCE
This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed, including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management (FICAM) Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. PII: Employing physical access controls that limit access to a facility that are commensurate with the level of sensitivity of the information processed in a facility protects the information from unauthorized access, use, and disclosure.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: , 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; FIPS Pub: 201; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A); 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(c); NIST SP: 800-73, 800-76, 800-78, 800-116; OMB Circular A-130: 7.g; Web: fips201ep.cio.gov, idmanagement.gov; IRS1075; CJIS 5.6	AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing physical access control; security plan; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; and other relevant documents or records.

PE-03(01): INFORMATION SYSTEM ACCESS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers).	
REFERENCES	**RELATED CONTROLS**
	PS-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; and other relevant documents or records.	

PE-03(02): FACILITY / INFORMATION SYSTEM BOUNDARIES

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers).	
REFERENCES	**RELATED CONTROLS**
	AC-4, SC-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; records of security checks; security audit reports; security inspection reports; facility layout documentation; information system entry and exit points; other relevant documents or records. Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for physical access control to the facility and/or information system; automated mechanisms supporting and/or implementing physical access control for the facility or information system; automated mechanisms supporting and/or implementing security checks for unauthorized exfiltration of information.	

PE-03(03): CONTINUOUS GUARDS / ALARMS / MONITORING

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CP-6, CP-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization employs one or more of the following to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week: guards; and/or alarms.
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; physical access control devices; facility surveillance records; facility layout documentation; information system entry and exit points; other relevant documents or records. Interview: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for physical access control to the facility where the information system resides; automated mechanisms supporting and/or implementing physical access control for the facility where the information system resides.

PE-04: ACCESS CONTROL FOR TRANSMISSION MEDIUM

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization controls physical access to network and information system distribution and transmission lines within organizational facilities using defined security safeguards.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS, CMS-MARS-E: Std.1 - Disable any physical ports (e.g., wiring closets, patch panels, etc.) not in use.	
SUPPLEMENTAL GUIDANCE	
Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in-transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1); 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.310(c); IRS1075; CJIS 5.6	MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility communications and wiring diagrams; and other relevant documents or records.	

PE-05: ACCESS CONTROL FOR OUTPUT DEVICES

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output	
CONTROL IMPLEMENTATION STANDARDS	
SPI:	

Std.1 - The applicant/bidder secures physical access to computer, paper, or other systems containing HHS Confidential Information from unauthorized personnel and theft (e.g., door locks, cable locks, laptops are stored in the trunk of the car instead of the passenger area, etc.).
SUPPLEMENTAL GUIDANCE
Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. PII: The access controls applied to output devices should be commensurate with the personally identifiable information (PII) confidentiality impact level. For example, human resource information is only sent to printers located in secured locations such as a locked suite.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(1), 45 C.F.R. §164.310(b), 164.310(c); OMB Circular A-130: 7.g; IRS1075; CJIS 5.6	PE-2, PE-3, PE-4, PE-18

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; actual displays from information system components; and other relevant documents or records. Examine: Information system restricts the use of unapproved output devices. Interview: Organizational personnel on physical access to information system output devices. Test: Automated mechanisms implementing restrictions on connecting unapproved output devices.

PE-06: MONITORING PHYSICAL ACCESS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs monthly and upon occurrence of security incidents or indications of potential events involving physical security; and c. Coordinates results of reviews and investigations with the organization's incident response capability. **CMS-MARS-E:** b. Reviews physical access logs weekly and upon occurrence of security incidents or indications of potential events involving physical security.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. PHI:	

Monitoring physical security incidents could identify PHI incidents or breaches.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; HIPAA: 45 C.F.R. §164.310(a)(2)(iii); 45 C.F.R. §164.308(a)(6)(i); IRS1075; CJIS 5.6	CA-7, IR-4, IR-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical access logs or records; and other relevant documents or records. Interview: Organizational personnel with physical access monitoring responsibilities.	

PE-06(01): INTRUSION ALARMS / SURVEILLANCE EQUIPMENT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization monitors physical intrusion alarms and surveillance equipment.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; and other relevant documents or records. Interview: Organizational personnel with physical access monitoring responsibilities. Test: Physical access monitoring capability.	

PE-06(04): MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization monitors physical access to the information system, in addition to the physical access monitoring of the facility, at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers).	
REFERENCES	**RELATED CONTROLS**
	PS-2, PS-3
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm/surveillance equipment logs or records; and other relevant documents or records. Interview: Organizational personnel with physical access monitoring responsibilities.

PE-08: VISITOR ACCESS RECORDS

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Maintains visitor access records to the facility where the information system resides except for those areas within the facility officially designated as publicly accessible for two (2) years; and b. Reviews visitor access records no less often than monthly. **IRS:** a. Maintain visitor access records to the facility where the information system resides for five (5) years. Also see Section 4.3, Restricted Area Access, for visitor access (AAL) requirements.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - At a minimum, visitor access records must include the following information: 1. Name and organization of the person visiting; 2. Visitor's signature; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited.	
SUPPLEMENTAL GUIDANCE	
Visitor access records include, for example, names and organizations of persons visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purposes of visits, and names and organizations of persons visited. Visitor access records are not required for publicly accessible areas. See NARA Schedule 18 for additional detail on this requirement. PHI: Visitor access records provide a history of who had access to facilities in the event of a privacy incident or breach. Records should be retained in accordance with the organization's records retention schedule.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **Federal:** IRS1075; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; and other relevant documents or records. Interview: Organizational personnel with responsibilities for reviewing physical access records.	

PE-08(01): AUTOMATED RECORDS MAINTENANCE / REVIEW

Priority: P3

Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; and other relevant documents or records. Interview: Organizational personnel with responsibilities for reviewing physical access records.	

PE-09: POWER EQUIPMENT AND CABLING

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization protects power equipment and power cabling for the information system from damage and destruction.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	
SUPPLEMENTAL GUIDANCE	
Organizations determine the types of protection necessary for power equipment and cabling employed at different locations, both internal and external, to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	PE-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; and other relevant documents or records.	

PE-10: EMERGENCY SHUTOFF

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;	

b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Implements and maintains a master power switch or emergency cut-off switch, prominently marked and protected by a cover, for data centers, servers, and mainframe rooms.	
SUPPLEMENTAL GUIDANCE	
This control applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	PE-15
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; and other relevant documents or records.	

PE-11: EMERGENCY POWER

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system and/or transition of the information system to a long-term alternate power source in the event of a primary power source loss.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	AT-3, CP-2, CP-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; and other relevant documents or records. Test: Uninterruptible power supply.	

PE-11(01): LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
CONTROL IMPLEMENTATION STANDARDS
Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.
SUPPLEMENTAL GUIDANCE
This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; and other relevant documents or records. Test: Alternate power supply.

PE-12: EMERGENCY LIGHTING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and covers emergency exits and evacuation routes within the facility.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.	
SUPPLEMENTAL GUIDANCE	
This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms.	

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	CP-2, CP-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; and other relevant documents or records. Interview: Organizational personnel with emergency planning responsibilities. Test: Emergency lighting capability.

PE-13: FIRE PROTECTION

Priority: P1

Baseline(s): Low, Low Plus, Moderate, high	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Information resources shall be protected from environmental hazards. Designated employees shall monitor equipment and shall be trained in environmental control procedures and in desired response in case of emergencies or equipment problems. **CMS-ARS:** Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements. Testing must comply with the previously mentioned recommendations, and be performed no less often than three (3) years.	
SUPPLEMENTAL GUIDANCE	
This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; and other relevant documents or records. Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.	

PE-13(01): DETECTION DEVICES / SYSTEMS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs fire detection devices/systems for the information system that activate automatically and notify defined personnel or roles (defined in the applicable security plan) and defined emergency responders (defined in the applicable security or safety plan) in the event of a fire.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection	

devices/systems; fire suppression and detection devices/systems documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems. Test: Simulated activation of fire detection devices/systems and automated notifications.

PE-13(02): SUPPRESSION DEVICES / SYSTEMS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to defined personnel (or roles) and defined emergency responders (defined in the applicable security or safety plan).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; and other relevant documents or records. Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems. Test: Simulated activation of fire suppression devices/systems and automated notifications.	

PE-13(03): AUTOMATIC FIRE SUPPRESSION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; and other relevant documents or records. Interview: Organizational personnel with responsibilities for fire detection and suppression devices/systems.	

PE-14: TEMPERATURE AND HUMIDITY CONTROLS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-specified levels; and
b. Monitors temperature and humidity levels within daily.

CMS-ARS:
c. Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS, CMS-MARS-E:
Low, Low Plus, Moderate, High:
Std.1 - Evaluate the level of alert and follow prescribed guidelines for that alert level.

Moderate, High:
Std.1 - Evaluate the level of alert and follow prescribed guidelines for that alert level.
Std.2 - Alert component management of possible loss of service and/or media.
Std.3 - Report damage and provide remedial action. Implement contingency plan, if necessary.

SUPPLEMENTAL GUIDANCE

This control applies primarily to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	AT-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; security plan; temperature and humidity controls; facility housing the information system; temperature and humidity controls documentation; temperature and humidity records; and other relevant documents or records.
Interview: Organization personnel with physical and environmental protection responsibilities.
Test: Simulated activation of fire suppression devices/systems and automated notifications.

PE-14(02): MONITORING WITH ALARMS / NOTIFICATIONS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing temperature and humidity monitoring; facility housing the information system; logs or records of temperature and humidity monitoring; records of changes to temperature and humidity levels that generate alarms or notifications; other relevant documents or records. Interview: Organizational personnel with responsibilities for information system environmental controls; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing temperature and humidity monitoring.

PE-15: WATER DAMAGE PROTECTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.	
SUPPLEMENTAL GUIDANCE	
This control applies primarily to facilities containing concentrations of information system resources, including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern without affecting entire organizations.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-5, CP-2	AT-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; and other relevant documents or records. Interview: Organization personnel with physical and environmental protection responsibilities. Test: Master water-shutoff valves; process for activating master water-shutoff.	

PE-15(01): AUTOMATION SUPPORT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts defined personnel or roles (defined in the applicable security plan).	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Tests the equipment on a schedule that complies with manufacturer recommendations and local, state, and federal requirements, no less often than three (3) years.	
SUPPLEMENTAL GUIDANCE	
Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.	
REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; and other relevant documents or records. Test: Automated mechanisms implementing master water shutoff valve activation.

PE-16: DELIVERY AND REMOVAL

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries. Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-6, AS-2; IRS1075	CM-3, MA-2, MA-3, MP-5, SA-12

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; security plan; facility housing the information system; records of items entering and exiting the facility; and other relevant documents or records. Interview: Organization personnel with responsibilities for controlling information system components entering and exiting the facility.

PE-17: ALTERNATE WORK SITE

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate work sites; b. Assesses, as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E:	

Std.1 - The organization defines management, operational, and technical information system security controls for alternate work sites. **IRS:** Std.1 - Alternate work sites may include, for example, government facilities or private residences of employees (see Section 4.7, Telework Locations, for additional requirements).
SUPPLEMENTAL GUIDANCE
Alternate work sites may include, for example, government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Organizations may define different sets of security controls for specific alternate work sites or types of sites, depending on the work-related activities conducted at those sites. This control supports the contingency planning activities of organizations and the federal telework initiative. PII: Personally Identifiable Information (PII) collected, stored, and processed at alternate worksite is subject to the same laws, regulations, and policies as PII handled at "non-alternate facilities."

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FISCAM: AS-5, CP-2; FedRAMP Rev. 4 Baseline; HIPAA: 45 C.F.R. §164.310(a)(2)(i); NIST SP: 800-46 OMB Memo: M-11-27, M-07-16, Att. 1 and Att. 4; IRS1075; CJIS 5.6	AC-17, CP-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; and other relevant documents or records. Interview: Organization personnel using alternate work sites.

PE-18: LOCATION OF INFORMATION SYSTEM COMPONENTS

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards, and to minimize the opportunity for unauthorized access.	
CONTROL IMPLEMENTATION STANDARDS	
IRS: Std.1 - For additional guidance, see Section 4.3, Restricted Area Access, and Section 4.5, Physical Security of Computers, Electronic, and Removable Media.	
SUPPLEMENTAL GUIDANCE	
Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). PHI: This control is required to limit intentional and unintentional disclosures of PHI in violation of the HIPAA Privacy and Security Rules.	

PII: This control is required to limit intentional and unintentional disclosures of personally identifiable information (PII) in violation of the Privacy Act. One example of an information system component requiring this control would be monitors; ensuring proper placement of the monitors will prevent unauthorized viewing. Another example of an information system component would be servers and disk arrays, and location would include ensuring these are in a secured space.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FISCAM: AS-5, CP-2; HIPAA: 45 C.F.R. §164.310(c); 45 C.F.R. §164.308(a)(3)(i); IRS1075; CJIS 5.6	CP-2, PE-19, RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; and other relevant documents or records.	

PE-18(01): FACILITY SITE

Priority: P3	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities and considers the physical and environmental hazards in its risk mitigation strategy.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	PM-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; and other relevant documents or records. Interview: Organization personnel with site selection responsibilities for the facility housing the information system.	

PE-19: INFORMATION LEAKAGE

Priority: P3	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The organization protects the information system from information leakage due to electromagnetic signals emanations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information leakage is the intentional or unintentional release of information to an untrusted environment from electromagnetic signals emanations. Security categories or classifications of information systems (with respect	

to confidentiality) and organizational security policies guide the selection of security controls employed to protect systems against information leakage due to electromagnetic signals emanations.	
REFERENCES	**RELATED CONTROLS**
Federal: FIPS Publication 199; HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms protecting the information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records. Interview: Organizational personnel with responsibilities for information system environmental controls; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing protection from information leakage due to electromagnetic signals emanations.	

PE-20: ASSET MONITORING AND TRACKING

Priority:	
Baseline(s):	Overlay(s): HIPAA, CJIS
CONTROL REQUIREMENTS	
The organization: a. Employs organization-defined asset location technologies to track and monitor the location and movement of organization-defined assets that store PHI within organizational-defined control areas; and b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. **CJIS:** a. Employs remote device location (GPS) tracking (if two other required advanced authentication compensating controls are not in place) to track and monitor the location and movement of agency-issued smartphones and tablets that process CJI and	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Asset location technologies can help organizations ensure that critical assets such as vehicles or essential information system components remain in authorized locations. Organizations consult with the Office of the General Counsel and the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) regarding the deployment and use of asset location technologies to address potential privacy concerns.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CM-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Physical and environmental protection policy; procedures addressing asset monitoring and tracking; asset location technologies and associated configuration documentation; list of organizational assets requiring tracking and monitoring; asset monitoring and tracking records; other relevant documents or records. Interview: Organizational personnel with asset monitoring and tracking responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for tracking and monitoring assets; automated mechanisms supporting and/or implementing tracking and monitoring of assets.	

(PL) PLANNING

The HHS organization requires the development, documentation, periodic update, and implementation of security plans for information systems within the HHS environment. HHS organization requires that those security plans describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

PL-01: SECURITY PLANNING POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls. b. Reviews and updates (as necessary) the current: 1. Security planning policy within every three (3) years; and 2. Security planning procedures within every three hundred and sixty five (365) days. **CMS-MARS-E:** b.1. Security planning policy within every three hundred and sixty five (365) days;	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency head or his/her designated representative(s) shall ensure that senior agency officials and information-owners, in collaboration with the Information Resources Manager and Chief Information Security Officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control. Std.2 - As required by TAC 202.23/73(a), the state organization delivers, at least annually, to the organization head a report on state organization information security program. Std.3 - PHI: The organization retains the policies and procedures in written form (which may be electronic) for 6 years from the date of its creation or the date when it was last in effect, whichever is later. The organization makes the documentation available to those persons responsible for implementing the procedures to which the document pertains.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PHI: Security planning addresses the requirements for confidentiality, availability, and integrity for the organization and individual information system(s).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC 202.20(3); DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(i); 45 C.F.R. §164.316(b)(2)(ii) HSPD 7: J(35); NIST SP: 800-12, 800-18, 800-100; IRS1075; CJIS 5.6	PM-9
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Security planning policy and procedures; and other relevant documents or records. Interview: Organizational personnel with security planning responsibilities.

PL-02: SYSTEM SECURITY PLAN

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops a security plan for the information system that is consistent with the HHS Procedures; and 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation. b. Distributes copies of the security plan and communicates subsequent changes to the plan to agency-defined personnel or roles; c. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and d. Updates the plan, minimally every three (3) years, to address current conditions or whenever: - There are significant changes to the information system/environment of operation that affect security; - Problems are identified during plan implementation or security control assessments; - When the data sensitivity level increases; - After a serious security violation due to changes in the threat environment; or - Before the previous security authorization expires. e. Protects the security plan from unauthorized disclosure and modification. **CMS-ARS:** PII: The system security plan (SSP) must provide the security category and the personally identifiable information (PII) confidentiality impact level of the system (as described in NIST SP 800-122), describe relationships with, and data flows of, PII to other systems, and provide an overview of security and privacy requirements for the system, including the security controls within the Privacy Overlays. The SSP must define the boundary within the system where PII is stored, processed, and/or maintained. The person responsible for meeting information system privacy requirements must provide input to the SSP. **IRS:** An approved and accurate SSR satisfies the requirements for the SSP (see Section 7.0, Reporting Requirements—6103(p)(4)(E)).	
CONTROL IMPLEMENTATION STANDARDS	
HIPAA: Std.1 - Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b)). **CMS-MARS-E:** Std.1 - When developing new system security plans or updating prior system security plans use the System Security Plan Template for ACA Administering Entity Systems, which can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	

Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in NIST 800-53 Appendix D and Committee on National Security Systems (CNSS) Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). NIST 800-53 Appendix I provides guidance on developing overlays.

Security plans need not be single documents; the plans can be a collection of various documents, including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference sufficient information to define what needs to be accomplished by those plans.

All HHS information systems and major applications should be covered by a security plan, which is compliant with current HHS procedures.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** E-Government Act of 2002 (Pub. L. No. 107-347) §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1; HIPAA: 45 C.F.R. §164.306(a); 45 C.F.R. §164.308(a)(1)(i); 45 C.F.R. §164.310; 45 C.F.R. §164.310(a)(2)(ii); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii) HSPD 7: J(35); NIST SP: 800-18; OMB Memo: M-03-22, M-07-16 Att. 1, A.2; IRS1075; CJIS 5.6	AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-4, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; and other relevant documents or records.
Interview: Organization personnel with security planning and plan implementation responsibilities for the information system.

PHI:
Examine: Sampling of policies and procedures relating to 164.306 for retention period. (See HIPAA 164.316(b))
Interview: Organizational personnel with retention responsibilities related to 164.306. (See HIPAA 164.316(b))

PII:
Examine: Procedures that document who obtains documentation and to whom documentation pertains for implementation.
Interview: Organizational personnel who are responsible for implementation of procedures to determine if documentation is available.

PL-02(03): PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization plans and coordinates security-related activities affecting the information system with affected internal or external stakeholders, groups, or organizations before conducting such activities in order to reduce the impact on other organizational entities.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
These stakeholders, groups, or organizations could include those involved with security-related activities, or providing services or support (such as [TIC or those involved in COOP planning). Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or non-urgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	CP-4, IR-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the information system; records of security plan reviews and updates; and other relevant documents or records. Interview: Organization personnel with security planning and plan implementation responsibilities for the information system.	

PL-04: RULES OF BEHAVIOR

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage, including: i. The HHS IS-Acceptable Use Policy (AUP) and HHS Acceptable Use Agreement; and ii. Any applicable HHS RoB; and iii. Any applicable system-specific RoB. b. Receives an acknowledgment (paper or electronic) from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior every three (3) years d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated. **CMS-MARS-E:** c. Reviews and updates the rules of behavior every three hundred sixty five (365) days **CMS-ARS** d. Requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated and at least every 365 days; e. Informs employees and contractors that the use of HHS information resources for anything other than authorized purposes set forth in the HHS RoB and Policy for Personal Use of Information Technology Resources	

is a violation of either or both of those policies, and is grounds for disciplinary action, monetary fines, and/or criminal charges that could result in imprisonment; and
f. Informs employees and contractors that the use of HHS information resources is subject to the HHS Policy for Monitoring Employee Use of HHS IT Resources

PII:
Pursuant to OMB M-07-16, organizational rules of behavior must include a policy outlining the rules of behavior to safeguard personally identifiable information (PII) and identifying consequences and corrective actions for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of PII involved.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - HHS shall develop a data use agreement (DUA) for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the department that relate to information security standards for state agencies.
Std.2 - The DUA must be updated at least biennially, but may update the agreement at any time as necessary to accommodate best practices in data management
Std.3 - Users of an information resource has the responsibility
a. Use the resource only for the purpose specified by the agency or information owner.
b. Comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction.
c. To formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his or her designated representative.

SPI:
Std.4 - The applicant/bidder requires Workforce members to formally acknowledge rules outlining their responsibilities for protecting HHS Confidential Information and associated systems containing HHS Confidential Information before their access is provided.

CMS-MARS-E:
Std.5 - The organization's rules of behavior are aligned with DHHS requirements posted at: http://www.hhs.gov/ocio/policy/hhs-rob.html

SUPPLEMENTAL GUIDANCE

This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users, including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures (or other electronic mechanisms) for acknowledging rules of behavior.

Rules of behavior are aligned with HHS requirements and made readily available.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** TAC 202.22(3); TGC 2054.134; DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HHS; Policy for Monitoring Employee Use of HHS IT Resources; HSPD 7: J(35); NIST SP: 800-18; OMB Memo: M-07-16, Att. 1, A.2. and Att. 4; IRS1075; CJIS 5.6	AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, AR-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; and other relevant documents or records. Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior

PL-04(01): SOCIAL MEDIA AND NETWORKING RESTRICTIONS

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): SPI, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) When organizational personnel are using such sites for official duties or in the conduct of official business; (ii) When organizational information is involved in social media/networking transactions; and (iii) When personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-18; IRS1075; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security planning policy; procedures addressing rules of behavior for information system users; rules of behavior; and other relevant documents or records. Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior.	

PL-07: SECURITY CONCEPT OF OPERATIONS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization: a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and b. Reviews and updates the CONOPS every three hundred and sixty five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents).	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	PL-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	

ASSESSMENT METHODS AND OBJECTS
Examine: Security planning policy; procedures addressing security CONOPS development; procedures addressing security CONOPS reviews and updates; security CONOPS for the information system; security plan for the information system; records of security CONOPS reviews and updates; other relevant documents or records. Interview: Organizational personnel with security planning and plan implementation responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for developing, reviewing, and updating the security CONOPS; automated mechanisms supporting and/or implementing the development, review, and update of the security CONOPS.

PL-08: INFORMATION SECURITY ARCHITECTURE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services. b. Reviews and updates (as necessary) the information security architecture no less often than every three (3) years and whenever changes are made to the enterprise architecture; c. Ensures that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions; and	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture.	

PII: The information security architecture identifies security and privacy controls necessary to support privacy requirements. The SAOP or CPO are the best resource for identifying privacy requirements and privacy controls.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. 107-347) §208; FedRAMP Rev. 4 Baseline; OMB Memo: M-03-22; CJIS 5.6	CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, AR-7, Appendix J
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; and other relevant documents or records.	

PL-09: CENTRAL MANAGEMENT

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization centrally manages organization-defined security controls and related processes.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Central management refers to the organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes. As central management of security controls is generally associated with common controls, such management promotes and facilitates standardization of security control implementations and management and judicious use of organizational resources. Centrally-managed security controls and processes may also meet independence requirements for assessments in support of initial and ongoing authorizations to operate as part of organizational continuous monitoring. As part of the security control selection process, organizations determine which controls may be suitable for central management based on organizational resources and capabilities. Organizations consider that it may not always be possible to centrally manage every aspect of a security control. In such cases, the security control is treated as a hybrid control with the control managed and implemented either centrally or at the information system level. Controls and control enhancements that are candidates for full or partial central management include, but are not limited to: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (all); CM-9 (1); CM-10; CM-11; CP-7 (all); CP-8 (all); SC-43; SI-2; SI-3; SI-7; and SI-8.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST Special Publication 800-37; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Security planning policy; procedures addressing security plan development and implementation; security plan for the information system; other relevant documents or records. Interview: Organizational personnel with security planning and plan implementation responsibilities; organizational personnel with responsibilities for planning/implementing central management of security controls and related processes; organizational personnel with information security responsibilities.	

Test: Organizational processes for central management of security controls and related processes; automated mechanisms supporting and/or implementing central management of security controls and related processes.

(PM) PROGRAM MANAGEMENT

The PM family provides controls for information security programs required by Federal Information Security Management Act (FISMA). This family, while not specifically referenced in FIPS 200, provides security controls at the organization level rather than the information system level.

PM-01: INFORMATION SECURITY PROGRAM PLAN

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. b. Reviews the organization-wide information security program plan within every three hundred sixty-five (365) days; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency head is responsible for the protection of information resources. Std.2 - The agency head shall a. Ensure that senior agency officials support the Chief Information Security Officer in developing, at least annually, a report on agency information security program, as specified in §202.21(b)(11) and §202.23(a). b. Review and approve at least annually the agency information security program required under TAC §202.24. Std.3 - The Chief Information Security Officer (CISO) shall: a. Report, at least annually, to the state agency head the status and effectiveness of security controls. b. Inform the parties in event of noncompliance TAC 202 and/or with the agency's information security policies. c. Develop and maintain an agency-wide information security plan as required by §2054.133, Texas Government Code. In developing the plan, the CISO shall: 1. Consider any vulnerability report prepared under TGC 2054.077 for the agency; 2. Incorporate the network security services provided by DIR to the agency under TGC 2059; 3. Identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information; 4. Identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction; 5. Include the best practices for information security developed by DIR or a written explanation of why the best practices are not sufficient for the agency's security; and 6. Omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems. 7. A written acknowledgement that the executive director or other head of the agency, the chief financial officer, and each executive manager as designated by the agency have been made aware of the risks revealed during the preparation of the agency's information security plan. d. Submit to the Texas Department of Information Resources a Biennial Information Security Plan, in accordance with §2054.133, Texas Government Code Std.4 - A review of the agency's information security program compliance with the DIR Security Controls Standard Catalog will be performed at least biennially, based on business risk management decisions, by	

individual(s) independent of the information security program and designated by the agency head or his or her designated representative(s).

SUPPLEMENTAL GUIDANCE

Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.
Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems.

PII:
The organization's approach to protection of personally identifiable information (PII) should be included in the information security program plan, including defining roles and responsibilities for protecting PII.

REFERENCES	RELATED CONTROLS
State: TAC 202.20(5); TAC 202.20(7); TAC 202.21(b)(1); TAC 202.21(b)(11); TAC 202.21(b)(12); TAC 202.23(b)(3); TAC 202.26(c); TGC 2054.133; DIR Security Control Standards Catalog **Federal:** 5 U.S.C. §552a(e)(10); FISMA (Pub. L. No. 107-347); OMB Circular A-130, 7.g.; 45 C.F.R. §164.308 (a)(1)(i); CJIS 5.6	PM-8, AR-1

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; and other relevant documents or records.
Interview: Organizational personnel with security planning and plan implementation responsibilities for the information security program.

PM-02: SENIOR INFORMATION SECURITY OFFICER

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, CMS-ARS, IRS, CMS-MARS-E, NCHHSTP, VA

CONTROL REQUIREMENTS

The organization appoints a Chief Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The head of the state agency or his/her designated representative(s) shall designate an Information Security Officer who has the explicit authority and the duty to administer the information security requirements of this chapter agency wide. Std.2 - The agency head shall ensure the Chief Information Security Officer: a. Reports to executive level management. b. Has authority for information security for the entire agency. c. Possesses training and experience required to administer the function described in TAC 202. d. Has information security duties as his/her primary duty. Std.3 - The CISO shall: a. Develop and maintain information security policies and procedures that address the requirements in TAC 202 and the agency's information security risks. b. Work with business and technical resources to ensure that controls are utilized to address all applicable requirements of TAC 202 and the agency's information security risks. c. Provide guidance and assistance to senior agency officials, information-owners, information custodians, and end users concerning their responsibilities.
SUPPLEMENTAL GUIDANCE
The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this official as the Senior Information Security Officer or Chief Information Security Officer. **HIPAA:** Assigning security responsibilities to a senior official supports the HIPAA Security Rule.

REFERENCES	RELATED CONTROLS
Texas HHS: Information Security and Privacy Inquiry Policy **State:** TAC 202.20(1); TAC 202.21(a); TAC 202.21(b)(2-3, 5); DIR Security Control Standards Catalog **Federal:** OMB Memo: M-05-08; 45 C.F.R. §164.308(a)(2); 45 C.F.R. §164.530(a); IRS1075	AR-1

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information security program policy; information security program plan; documentation addressing roles and responsibilities of the Chief Information Security Officer position; information security program mission statement; and other relevant documents or records. Interview: CISO or designated representative.

PM-03: INFORMATION SECURITY RESOURCES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency head or his/her designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the agency head. Std.2 - The Chief Information Security Officer (CISO) shall report, at least annually, to the agency head on agency information security requirements and requests.	
SUPPLEMENTAL GUIDANCE	

Organizations consider establishing champions for information security efforts and as part of including the necessary resources, assign specialized expertise and resources as needed. Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process PII: Ensuring that information security is adequately resourced supports the implementation of all security-related privacy requirements.	
REFERENCES	**RELATED CONTROLS**
State: TAC 202.20(2); TAC 202.23(a)(3); DIR Security Control Standards Catalog **Federal:** E-Government Act of 2002 (Pub. L. No. 107-347), §208; NIST SP: 800-65	PM-4, SA-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information security program policy; capital planning and investment policy; procedures addressing management and oversight for information security-related aspects of the capital planning and investment control process; capital planning and investment documentation; documentation of exceptions supporting capital planning and investment requests; business cases; Exhibit 300; Exhibit 53; and other relevant documents or records. Interview: Organizational personnel managing and overseeing the information security-related aspects of the capital planning and investment control process.	

PM-04: PLAN OF ACTION AND MILESTONES PROCESS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems: 1. Are developed and maintained; 2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. If applicable, are reported in accordance with OMB FISMA reporting requirements and other applicable requirements, such as those within the FedRAMP. b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The state organization develops and updates, a plan of action and milestone process for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls in order to reduce or eliminate known vulnerabilities in the system. **CMS-MARS-E** Std.2 - CMS Reporting Requirement: AEs must submit copies of their updated POA&M to CMS on a quarterly basis. The POA&M template (an Excel spreadsheet) used to report the status of POA&M can be found at: https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/	
SUPPLEMENTAL GUIDANCE	
The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. With the increasing emphasis on organization-wide risk management across all three tiers in the risk management hierarchy (i.e., organization, mission/business process, and information system), organizations view plans of action and milestones from an organizational perspective, prioritizing risk response actions and ensuring consistency with the goals and objectives of the organization. Plan of action and milestones updates are based on findings from security control assessments and	

continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-02-01, M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.310(d)	CA-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information security program policy; plan of action and milestones policy; procedures addressing plan of action and milestones process; plan of action and milestones for the security program; plan of action and milestones for organizational information systems; other relevant documents or records.	

PM-05: INFORMATION SYSTEM INVENTORY

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops and maintains an inventory of its information systems, to include those operated on behalf of other Federal requirements (e.g., for CMS, IRS, SSA, etc. by a contractor, vendor, cloud service provider, or other service provider).	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - No later than December 1 of each odd-numbered year, a state agency shall complete a review of the agency's information resources that includes: a. An review of the inventory of the agency's major information systems and other operational or logistical components related to deployment of information resources; b. An inventory of the agency's major databases and applications; and c. A description of the agency's existing and planned telecommunications network configurations. Std.2 - The Chief Information Security Officer (CISO) shall review the agency's inventory of information systems and related ownership and responsibilities.	
SUPPLEMENTAL GUIDANCE	
This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements. For specific information system inventory reporting requirements, organizations consult OMB annual FISMA reporting guidance. OMB Circular NO A-130 Appendix III The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. PII: Maintaining a current information system inventory supports privacy by informing personally identifiable information (PII) inventories, data flows, and generally assists in monitoring the maintenance and use of PII. **HIPAA:** Information system inventory should govern the receipt and removal of hardware and electronic media that contains PHI.	
REFERENCES	**RELATED CONTROLS**
State: TAC 202.21(b)(7); TGC 2054.0965; DIR Security Control Standards Catalog **Federal:** http://www.omb.gov	SE-01
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Inventory of information systems.

PM-06: INFORMATION SECURITY MEASURES OF PERFORMANCE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops, monitors, and reports on the results of information security measures of performance to evaluate the effectiveness of IT security and privacy policies, procedures, and controls. The measures and metrics must provide information on measures of implementation, efficiency, effectiveness, and impact.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The Chief Information Security Officer shall report, at least annually, to the agency head on the effectiveness of current information security program and status of key initiatives;	
SUPPLEMENTAL GUIDANCE	
Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.	
REFERENCES	**RELATED CONTROLS**
State: TAC 202.23(a)(1); DIR Security Control Standards Catalog **Federal:** NIST SP: 800-55	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: List of monitored security measures of performance; reports providing results of security measure monitoring. Examine: Verify that reported measures and metrics provide at least measures of implementation, efficiency, effectiveness, and impact for each measure of performance. Interview: Organizational personnel with security performance measurement responsibilities.	

PM-07: ENTERPRISE ARCHITECTURE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops and implements an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture (FEA). The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This process of security requirements integration also embeds into the enterprise architecture, an integral information security architecture consistent with organizational risk management and information security strategies. For PM-7, the information security architecture is developed at a system-of-systems level (organization-wide), representing all of the organizational information systems. For PL-8, the information security architecture is developed at a level representing an individual information system, but at the same time is consistent with the information security architecture defined for the organization. Security requirements and security control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures.	

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); FISMA (Pub. L. No. 107-347); NIST SP: 800-39; OMB Circular A-130, 7.g.; Web: fsam.gov; 45 C.F.R. §164.308(a)(1)(i)	PL-2, PL-8, PM-11, RA-2, SA-3, AR-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Enterprise architecture design documentation; enterprise architecture implementation documentation; enterprise architecture requirements documentation; enterprise architecture risk assessment documentation; and other relevant documentation.
Interview: Organizational personnel with enterprise architecture design and/or conformance responsibilities.

PM-08: CRITICAL INFRASTRUCTURE PLAN

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Protection strategies are based on the prioritization of critical assets and resources. The requirements and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

REFERENCES	RELATED CONTROLS
Federal: NIST SP 800-34, 800-60	PM-1, PM-9, PM-11, RA-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program policy; critical infrastructure and key resources protection plan; protection plan development documentation; other relevant documents or records.
Interview: Organizational personnel with critical infrastructure and key resources protection plan responsibilities.

PM-09: RISK MANAGEMENT STRATEGY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and
use of information systems;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the risk management strategy at least every three hundred and sixty-five (365) days or as required, to address organizational changes.

CMS-ARS:
PII: The risk management strategy must include a process to evaluate and address privacy risks for individuals and information (data) such as risk to individual, risk to the system, risk to the organization, and risk to the

enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The Chief Information Security Officer shall report, at least annually, to the agency head on residual risks identified by the agency risk management process.
Std.2 - The state organization head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity.
Std.3 - The state organization head or his or her designated representative(s) shall approve the security risk management plan. This information may be exempt from disclosure under §2054.077(c), Government Code.
Std.4 - The CIO of HHS shall prepare or have prepared a biennial report, not later than October 15 of each even-numbered year, including an executive summary of the findings of the report, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.
Std.5 - Separate from the executive summary described by Std.4, HHS shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

HIPAA:
Std.4 - The risk management strategy must include a process to evaluate and address privacy risks for individuals and PHI such as risk to individual, risk to the system, risk to the organization, and risk to the enterprise. In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.

SUPPLEMENTAL GUIDANCE

An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive.

PII:
A comprehensive risk management strategy includes privacy as an input where appropriate to ensure privacy risks to individuals and organizations are identified, prioritized, and managed consistently across the organization's business processes, programs, and systems.

REFERENCES	RELATED CONTROLS
State: TAC 202.23(a)(2); TAC 202.25; TGC 2057.077; DIR Security Control Standards Catalog **Federal:** NIST SP: 800-30, 800-39; OMB Memo: M-03-22, M-06-16, M-07-16 Att. 1, B.1 and Att. 2, A.1; OMB Circular A-130, 7.g.; 45 C.F.R. §164.308(a)(1)(ii); 45 C.F.R. §164.316(a)	RA-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program policy; risk management strategy documentation; evidence of consistent implementation of risk management strategy; samples of risk management documentation from disparate organizational information systems; other relevant documents or records.
Interview: Organizational personnel with risk management strategy responsibilities.

PM-10: SECURITY AUTHORIZATION PROCESS

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Fully integrates the security authorization processes into an organization-wide risk management program.

CMS-ARS:
PII: The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements, such as privacy impact assessments (PIA) and systems of records notices (SORN) when applicable, have been appropriately addressed prior to any security authorization.

CMS-MARS-E:
d. The Administering Entity's Authorizing Official:
1. Grants/denies the Authorization To Operate (ATO) based on the evaluation of security risks;
2. Manages the CMS-established Authority to Connect (ATC) process;
3. If the organization maintains a system-to-system connection with CMS through an executed Interconnection Security Agreement with CMS, CMS grants/denies the "Authority to Connect"; and
4. Grants/denies the authorization to establish system-to-system connections with other external entities.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - The organization's security authorization process must ensure privacy safeguards and privacy documentation requirements have been appropriately addressed prior to any security authorization.

SUPPLEMENTAL GUIDANCE

Security authorization processes for information systems and environments of operation require the implementation of an organization-wide risk management process, a Risk Management Framework, and associated security standards and guidelines. Specific roles within the risk management process include an organizational risk executive (function) and designated authorizing officials for each organizational information system and common control provider. Security authorization processes are integrated with organizational continuous monitoring processes to facilitate ongoing understanding and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.

PII:
The security authorization process provides a means for evaluating whether a system/process has met given privacy safeguards and documentation requirements.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208; NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g. and 8.b.(3); 45 C.F.R. §164.308(a)(2)	CA-6, AR-2, AR-7, TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); and other relevant documents or records.
Interview: Organizational personnel with security authorization responsibilities for information systems; organizational personnel with risk management responsibilities.
Test: Organizational processes for security authorization; automated mechanisms supporting the security authorization process.

PM-11: MISSION/BUSINESS PROCESS DEFINITION

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. **CMS-ARS:** c. Fully integrates the security authorization processes into an organization-wide risk management program. PII: When defining mission/business processes for information security and identifying resulting risks, the organization must address the privacy risks stemming from those processes.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. PII: In addition to business risks that arise out of privacy violations, such as reputation or liability risks, organizational policies should also focus on minimizing the risk of harm to individuals.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FIPS Pub: 199; NIST SP: 800-60; OMB Circular A-130: 7.g. and 8.b.(1)(b), 8.b.(2)(b), and Appendix IV; 45 C.F.R. §164.306(a) and (b)	PM-7, PM-8, RA-2, AR-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information security program policy; mission/business process definitions; mission/business process risk assessment documentation; other relevant documents or records. Interview: Organizational personnel with mission/business process definition responsibilities.	

PM-12: INSIDER THREAT PROGRAM

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team. PII: When defining the requirements for and designing an organization's insider threat program, the insider threat team must engage the participation, and obtain concurrence, of the organization's Privacy Officer prior to implementation. For existing insider threat programs, conduct a review of the program with the organization's Privacy Officer to ensure program meets applicable privacy requirements.	
CONTROL IMPLEMENTATION STANDARDS	

Std.1 - As required by HHS Policy, the organization implements the insider threat program in accordance with HHS Policy for Monitoring Employee Use of HHS IT Resources.
SUPPLEMENTAL GUIDANCE
Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture. Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines. PII: The privacy risks inherent with aggregating sensitive personally identifiable information (PII) from multiple data resources within an organization, such as human resource and background investigation information, and the potential for scope creep require the active participation, review, and concurrence of the Privacy Officer.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(5), (9), (10); E-Government Act of 2002 (Pub. L. No. 107-347), §208; Executive Order: 13587; HHS: Policy for Monitoring Employee Use of HHS IT Resources; OMB Memo: M-07-16; OMB Circular A-130: 7.g.	AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-1, PM-14, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information security program policy; risk management policy; procedures addressing incident handling and response; and other relevant documents or records. Interview: Organizational personnel with risk management responsibilities, organizational personnel with incident response responsibilities.

PM-13: INFORMATION SECURITY WORKFORCE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization establishes an information security workforce development and improvement program.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency head or his/her designated representative(s) shall ensure that the agency has trained personnel to assist the agency in complying with the requirements of TAC 202 and related policies.	
SUPPLEMENTAL GUIDANCE	
Information security workforce development and improvement programs include, for example:	

(i) Defining the knowledge and skill levels needed to perform information security duties and tasks;
(ii) Developing role-based training programs for individuals assigned information security roles and responsibilities; and
(iii) Providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions. Such workforce programs
can also include associated information security career paths to encourage:
a. Information security professionals to advance in the field and fill positions with greater responsibility; and
b. Organizations to fill information security-related positions with qualified personnel. Information security workforce development and improvement programs are complementary to organizational security awareness and training programs. Information security workforce development and improvement programs focus on developing and institutionalizing core information security capabilities of selected personnel needed to protect organizational operations, assets, and individuals.

PII:
To implement adequate security controls, the organization's information security and privacy workforce should be knowledgeable of the applicable privacy and security requirements commensurate with the level of access or responsibility for applying appropriate safeguards. The information security workforce should receive role-based training for the privacy requirements commensurate with the level of access or responsibility for applying safeguards to personally identifiable information (PII).

REFERENCES	RELATED CONTROLS
State: TAC 202.20(4); DIR Security Control Standards Catalog **Federal:** HHS Memorandum: Role-Based Training (RBT) of Personnel with Significant Security; Responsibilities; Code: 5 U.S.C. §552a(e)(9)-(10); OMB Memo: M-07-16; OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(2)	AT-2, AT-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Information security program policy; security workforce development and improvement program; security workforce development and improvement program procedures; and other relevant documents or records.
Examine: Information system implements automated information security and privacy role-based training/staff participation tracking.
Interview: Organizational personnel with risk management responsibilities, organizational personnel with security workforce development program responsibilities.

PM-14: TESTING, TRAINING, AND MONITORING

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
1. Are developed and maintained; and
2. Continue to be executed in a timely manner.
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

CMS-ARS:
PII: Reviews testing, training and monitoring plans for consistency with the organizational privacy risk management strategy.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of

continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments. PII: It is critical to integrate privacy risk management, compliance monitoring, and testing into the organizational risk management strategy and the associated testing and training requirements otherwise an important aspect of privacy may be overlooked.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9)-(10); Pub. L. No. 107-347, §208; HHS: Role-Based Training (RBT) of Personnel with Significant Security Responsibilities; NIST SP: 800-16, 800-37, 800-115, 800-137; OMB Memo: M-07-16 Att.1, A.2., M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g.	AT-3, CA-7, CP-4, IR-3, SI-4, AR-4, AR-5, DM-3, SE-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; and other relevant documents or records. Interview: Organizational personnel with information security responsibilities. Test: Automated mechanisms supporting development and maintenance of plans and processes for conducting security testing, training, and monitoring activities.	

PM-15: CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Priority: P3	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; OMB Memo: M-07-16, M-05-08; OMB Circular A-130: 7.g.	SI-5, AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Information security program policy; security testing, training, and monitoring process documentation; security testing, training, and monitoring activities procedures; and other relevant documents or records.

PM-16: THREAT AWARENESS PROGRAM

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization implements a threat awareness program that includes a cross-organization information-sharing capability	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** Cybersecurity Enhancement Act of 2104	IR-10, PM-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information security program policy; threat awareness program policy; threat awareness program procedures; and other relevant documents or records. Interview: Security Operations personnel to verify the organization is actively participating in the threat awareness program of CMS. Verify that personnel act on threat information received from HHS Information Security (and other external sources) as well as reporting threat information derived from investigations (or other external sources) to HHS Information Security.	

(PS) PERSONNEL SECURITY

The HHS organization works with human resources to (i) ensure that individuals occupying positions of responsibility within HHS (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that HHS information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with HHS security policies and procedures.

PS-01: PERSONNEL SECURITY POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
b. Reviews and updates (as necessary) the current:
1. Personnel security policy within three (3) years; and
2. Personnel security procedures within every three hundred and sixty five (365) days.

CMS-ARS:
PII:
The personnel security policies and procedures must address the different levels of background investigations, or other personnel security requirements, necessary to access different levels of personally identifiable information (PII).

CMS-MARS-E:
b.1. Personnel security policy within three hundred and sixty five (365) days

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PII:
Roles that require access to certain types of sensitive information, such as PII may require additional personnel security measures beyond those applied to the general workforce of an organization.
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B); 45 C.F.R. §164.316(a); 45 C.F.R. §164.316(b)(1)(i); 45 C.F.R. §164.316(b)(2)(ii) NIST SP: 800-12, 800-100; OMB Memo: M-07-16, Att. 4; OMB Circular A-130: 7.g. and 8.a.1(f); IRS1075; CJIS 5.6	PM-9

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy and procedures; and other relevant documents or records.

PS-02: POSITION RISK DESIGNATION

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions;
c. Reviews and, if necessary, updates position risk designations at least every three (3) years or whenever a position's duties are changed/revised/realigned, and ensures that these risk designations are consistent with HHS policy and guidance.

CMS-ARS:
d. Ensures that all individuals with significant security responsibilities possess, at a minimum, a Level 5 Public Trust;
e. Ensures that individuals are designated to position-sensitivity levels that are commensurate with the responsibilities and risks associated with the position; and

PII:
Whether a member of the workforce will be working with personally identifiable information (PII) is a factor in determining the screening criteria for working in the position.

CMS-MARS-E, IRS:
c. Reviews and, if necessary, updates position risk designations at least every three hundred sixty-five (365) days or whenever a position's duties are changed/revised/realigned, and ensures that these risk designations are consistent with HHS policy and guidance.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - All authorized users (including, but not limited to, state organization personnel, temporary employees, and employees of independent contractors) of the state organization's information resources, shall formally acknowledge that they will comply with the security policies and procedures of the state organization or they shall not be granted access to information resources. The state organization head or his or her designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to state organization information resources.

IRS:
Std.2 – Comply with IRS1075 Section 5.1.1 Background Investigation Minimum Requirements

CJIS:
Std.2 – Comply with CJIS Security Policy Section 5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI and 5.12.1.2 Personnel Screening for Contractors and Vendors

SUPPLEMENTAL GUIDANCE

Position risk designations reflect HHS policy and guidance. Risk designations can guide and inform the types of authorizations individuals receive when accessing organizational information and information systems. Position screening criteria include explicit information security role appointment requirements (e.g., training, security clearances).

PHI:
Under HIPAA, this is an addressable control.

PII:
Position risk designations, for different levels of access to sensitive information such as PII should be commensurate with the risks associated with the confidentiality impact level for the information.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; HHS HR Manual **State:** DIR Security Control Standards Catalog **Federal:** 5 C.F.R. 731.106; IRS1075; CJIS 5.6	AT-3, PL-2, PS-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; and other relevant documents or records.

PS-03: PERSONNEL SCREENING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Screens individuals prior to authorizing access to the information system; b. Rescreens individuals as applicable periodically, consistent with the risk designation of the position. **CMS-MARS-E:** c. When an employee moves from one position to another, the higher level of clearance should be adjudicated. **CMS-ARS:** b. Rescreens individuals periodically and anytime they move to a new position with a higher risk designation; c. Conducts background investigations in a manner commensurate with OPM, HHS, and CMS HR policy and guidance; d. Performs reinvestigations in accordance with guidance provided by current personnel security policy; and e. Refuses employees and contractors access to information systems until they have: 1. Been granted an interim clearance; and 2. Signed the appropriate access agreements	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The organization performs a criminal history check for all persons prior to employment. Std.2 - The organization requires all employees and contractors who have access to ACA-sensitive information to meet personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum, contacting references provided by the employee as well as the local law enforcement agency or agencies. **CMS-ARS:** Std.1 - Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust sensitivity level clearance as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook. **CJIS:** Std. 1 - To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. Std.2 - Must comply with CJIS Personnel Security Policy and Procedures. See CJIS 5.6 for further information.	
SUPPLEMENTAL GUIDANCE	
Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems. PHI: Under HIPAA, this is an addressable control. PII: Screening individuals who are provided access to sensitive information, such as PII, and re-screening as deemed appropriate by CMS or the organization, reduces risk.	

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; HHS HR Manual **State:** DIR Security Control Standards Catalog **Federal:** 5 C.F.R. 731.106; FIPS Publications 199, 201; NIST Special Publications 800-60, 800-73, 800-76, 800-78; ICD 704; IRS1075; CJIS 5.6	AC-2, IA-4, PE-2, PS-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; and other relevant documents or records.

PS-03(01): CLASSIFIED INFORMATION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	AC-3, AC-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities.
Test: Organizational processes for clearing and indoctrinating personnel for access to classified information.

PS-03(02): FORMAL INDOCTRINATION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The organization ensures that individuals accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, are formally indoctrinated for all of the relevant types of information to which they have access on the system.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Types of classified information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI).

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	AC-3, AC-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; other relevant documents or records. Interview: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities. Test: Organizational processes for formal indoctrination for all relevant types of information to which personnel have access.

PS-03(03): INFORMATION WITH SPECIAL PROTECTION MEASURES

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection: a. Have valid access authorizations that are demonstrated by assigned official government duties; and b. Satisfy additional personnel screening periodically, consistent with the sensitivity of the information being accessed.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
PHI: Under HIPAA, this is an addressable control. PII: Access to sensitive information, such as personally identifiable information (PII) and protected health information (PHI), requires both a valid need to know as documented by an access authorization request, and requires a background investigation (or appropriate screening) to ensure the individual being provided access is suitable.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 C.F.R. §731.106; FedRAMP Rev. 4 Baseline; OMB Memo: 16-04; 45 C.F.R. §164.308(a)(3)(ii)(B) ; CJIS 5.6	AR-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; list of assigned official government duties for each user of the system; and other relevant documents or records. Interview: Organizational personnel with personnel screening responsibilities; system users.	

PS-04: PERSONNEL TERMINATION

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization, upon termination of individual employment: a. Disables information system access in accordance with Implementation Standard 1; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; f. Notifies defined personnel or roles (defined in the applicable security plan) immediately; and	

CMS-ARS, CMS-MARS-E:
g. Immediately escorts employees terminated for cause out of the organization.

CONTROL IMPLEMENTATION STANDARDS

Low, Low Plus:
Std.1 - System access must be revoked during the employee termination process/action.

Moderate, High:
Std.1 - System access must be revoked prior to or during the employee termination process/action.

CMS-ARS, CMS-MARS-E:
Std.2 - All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).

SUPPLEMENTAL GUIDANCE

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified.
Appropriate personnel have access to official records created by terminated employees that are stored on information systems.

PHI:
Under HIPAA, this is an addressable control.

PII:
This control governs termination procedures for access to sensitive information, such as personally identifiable information (PII).

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; HHS HR Manual **State:** DIR Security Control Standards Catalog **Federal:** IRS1075; CJIS 5.6	AC-2, IA-4, PE-2, PL-4, PS-5, PS-6

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; and other relevant documents or records.

PS-04(02): AUTOMATED NOTIFICATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization employs automated mechanisms to notify defined personnel/roles as designated by the organization (e.g., Human Resources, managers/supervisors, system administrators, physical security personnel) upon termination of an individual.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - If automated mechanisms are not feasible, a manual and documented process must be in place consistent with the baseline PS-4(f) control.

SUPPLEMENTAL GUIDANCE

In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; and other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities.

PS-05: PERSONNEL TRANSFER

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates a review of required system access immediately upon reassignment or transfer;
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies the information custodian immediately upon reassignment or transfer.

CMS-ARS, CMS-MARS-E:
b. Initiates the following transfer or reassignment actions during the formal transfer process:
1. Re-issuing or confirming the need to continue to have/access appropriate information system-related property (e.g., keys, identification cards, building passes);
2. Notification to security management;
3. Closing obsolete accounts and establishing new accounts; and
4. When an employee moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed 30 days.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Cloud
Std.1 - For cloud service providers, the organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates organization-defined transfer or reassignment actions within five (5) days following the formal transfer action.
Std.2 - For cloud service providers, the organization defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.

SUPPLEMENTAL GUIDANCE

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted. Organizations define actions appropriate for the types of reassignments or transfers, whether permanent or extended. Actions that may be required for personnel transfers or reassignments to other positions within organizations include, for example:
(i) Returning old and issuing new keys, identification cards, and building passes;
(ii) Closing information system accounts and establishing new accounts;
(iii) Changing information system access authorizations (i.e., privileges); and
(iv) Providing for access to official records to which individuals had access at previous work locations and in previous information system accounts.

PHI:
Under HIPAA, this is an addressable control.

PII:
When personnel are reassigned or transferred, their access to sensitive information, such as PII, must be reviewed to determine whether and how their access permissions should change.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; HHS HR Manual **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b)(1) and (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(C); 45 C.F.R. §164.308(a)(3)(ii)(B); IRS1075; CJIS 5.6	AC-2, IA-4, PE-2, PS-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of information system and facility access authorizations; and other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities.

PS-06: ACCESS AGREEMENTS

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every 365 days, whichever occurs first; and
c. Ensures that individuals requiring access to organizational information and information systems:
1. Acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and
2. Re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated or within every 365 days.

CMS-MARS-E:
a. The organization develops and documents access agreements for organizational information systems, consistent with the provisions of the ACA and the requirements of 45 CFR §155.260 – Privacy and security of personally identifiable information, paragraphs (b)(2) and (c).

CONTROL IMPLEMENTATION STANDARDS

Std.1 - HHS shall develop a data use agreement (DUA) for use by the agency that meets the particular needs of the agency and is consistent with rules adopted by the department that relate to information security standards for state agencies.

SUPPLEMENTAL GUIDANCE

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy.

The HHS AUA is the standard HHS access agreement. All new users of HHS, including CMS, information resources must read the HHS AUA and sign the accompanying acknowledgement form before accessing Department data or other information, systems, and/or networks. This acknowledgement must be completed every 365 days thereafter, which may be done as part of annual the organization Information Systems Security Awareness Training (see AT-3).

PII: Examples of access agreement documents required for access to personally identifiable information (PII) may include access authorization requests, nondisclosure agreements, acceptable use agreements, privacy training and awareness, and rules of behavior.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy; HHS Data Use Agreement **State:** TGC 2054.134; DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-4, SD-1, SD-2, SM-4; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R. §164.308(a)(3)(ii)(B), 45 C.F.R. §164.308(a)(4)(ii)(B), 45 C.F.R. §164.310(b), 45 C.F.R. §164.310(d)(2)(iii), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a) OMB Memo: M-07-16 Att. 1, A.2. and Att. 4; IRS1075; CJIS 5.6	AC-2, PL-4, PS-2, PS-3, PS-4, PS-8, AR-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; security plan; access agreements; records of access agreement reviews and updates; and other relevant documents or records. Interview: Organizational personnel with personnel security responsibilities.	

PS-06(02): CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization ensures that access to classified information requiring special protection is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; (b) Satisfy associated personnel security criteria; and (c) Have read, understood, and signed a nondisclosure agreement.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Classified information requiring special protection includes, for example, collateral information, Special Access Program (SAP) information, and Sensitive Compartmented Information (SCI). Personnel security criteria reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; access agreements; access authorizations; personnel security criteria; signed nondisclosure agreements; other relevant documents or records. Interview: Organizational personnel with personnel security responsibilities; organizational personnel who have signed nondisclosure agreements; organizational personnel with information security responsibilities. Test: Organizational processes for access to classified information requiring special protection.	

PS-07: THIRD-PARTY PERSONNEL SECURITY

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify the HHS Contract Manager of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges immediately upon personnel transfer or termination; and
e. Monitors provider compliance.

CMS-MARS-E:
d. The organization requires third-party providers to notify Contracting Officers or Contracting Officer's Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.

CMS-ARS:
d. Requires third-party providers to notify Contracting Officers or Contracting Officer Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges as soon as possible within a maximum of (72 hours High, seven (7) calendar days Moderate, or 30 calendar days Low) from the formal termination action.

CONTROL IMPLEMENTATION STANDARDS

SPI:
Std.1 - The applicant/bidder must be willing to perform or submit to a criminal background check on Authorized Users.

CMS-ARS, CMS-MARS-E:
Std.1 - Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.

SUPPLEMENTAL GUIDANCE

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated.

PII:
This control ensures that third-party service providers that will have access to sensitive information, such as personally identifiable information (PII), are held accountable in the same way the organizational personnel are held accountable.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(m); Federal Acquisition Regulation (FAR): Parts 24.1, 39.105, 52.224-1&2; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4, SM-7; HIPAA: 45 C.F.R. §164.308(a)(3)(ii)(A), 45 C.F.R.	PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21, AR-3

§164.308(a)(4)(ii)(B), 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); 45 C.F.R. §164.314(a); NIST SP: 800-35; OMB Circular A-130: 7.g., 8.a.1(f); IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; and other relevant documents or records.
Interview: Organizational personnel with personnel security responsibilities; third-party providers.

PS-08: PERSONNEL SANCTIONS

Priority: P3	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies employee manager immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

CMS-ARS:
b. Notifies applicable management within defined time period, not to exceed (three (3) High, seven (7) Moderate, or thirty (30) for Low) calendar days, when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of General Counsel regarding matters of employee sanctions.

PII:
If the personnel sanctions are associated with the loss, theft, or compromise of personally identifiable information (PII), additional care must be taken to prevent further privacy breach. When providing notice of sanctions, do not provide the PII involved in the incident to anyone without an explicit need to know. Unless the individual needs the specific PII elements breached to perform their job function, the individual does not need to know the PII. Instead, provide characterization of the type(s) of PII breached, e.g., provide “Full Name” instead of providing “John Doe,” or “Blood Type” instead of “A positive.”

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(9); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-4; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(C); OMB Memo: M-07-16 Att. 2, A.2., Att. 4; IRS1075; CJIS 5.6	PL-4, PS-6

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; and other relevant documents or records. Interview: Organizational personnel with personnel security responsibilities.

(RA) RISK ASSESSMENT

The HHS organization requires that risks to HHS operations (including its mission, functions, image, or reputation), HHS assets, and individuals, resulting from the operation of HHS information systems and the associated processing, storage, or transmission of HHS information, are assessed.

RA-01: RISK ASSESSMENT POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls on information systems and paper records; and b. Reviews and updates (as necessary) the current: 1. Risk assessment policy within every three (3) years and 2. Risk assessment procedures within every three hundred and sixty five (365) days. **CMS-MARS-E:** b.1. Risk assessment policy within every three hundred and sixty five (365) days PII: Organization risk assessment policy and procedures must incorporate the requirements to conduct information system privacy risk management processes across the life cycle of an information system collecting, using, maintaining, and/or disseminating personally identifiable information (PII).	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The agency shall, in consultation with the agency Information Resource Manage and Chief Information Security Officer (CISO), identify information owners, custodians, and user of information resources. Std.2 - The information owners, custodians, and users' responsibilities should be defined and documented by the agency. Std.3 - The state organization has a risk assessment policy which includes process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on an organization's mission, functions, image, reputation, assets, or individuals.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. PII: The Privacy Office (Senior Official for Privacy) should be consulted with in developing risk assessment policy and procedures to cover information systems containing PII.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC 202.20(6); TAC 202.21(a)(2); TAC 202.22; DIR Security Control Standards Catalog	PM-2, PM-9, AR-2

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a); NIST SP: 800-12, 800-30, 800-100; OMB Circular A-130: 7.g. and 8.b.(3)(b); OMB Memo: M-07-16 Att. 1, A.2., M-05-08; IRS1075	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy and procedures; and other relevant documents or records.
Interview: Organizational personnel with risk assessment responsibilities.

RA-02: SECURITY CATEGORIZATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Categorizes information and the information system in accordance with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The Information Owner or his or her designated representative(s) are responsible for classifying information under their authority, with the concurrence of the state agency head or his or her designated representative(s), in accordance with agency's established information classification categories.
Std.2 - State organizations are responsible for defining all information classification categories except the Confidential Information category, which is defined in Subchapter A of this chapter, and establishing the appropriate controls for each.
Std.3 - Involve the Senior Official for Privacy, or their designee, when conducting the security categorization process for information systems containing personally identifiable information (PII) or protected health information (PHI).

SUPPLEMENTAL GUIDANCE

Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/Information Owner(s)/Custodian(s), and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives (HSPD), potential national-level adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted.
All HHS information systems categorized as High, Moderate, or Low-Plus are considered sensitive or contain sensitive information. All HHS information systems categorized as Low are considered non-sensitive or contain non-sensitive information. Organizations implement the minimum security requirements and controls as established in the current HHS Information Security Standard, based on the system security categorization.

PII:
A determination of security categorization is based in part on whether the information is PII, or the system contains sensitive information such as PII, and is a fundamental determination for implementing security controls.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC202.22(1)(A); DIR Security Control Standards Catalog	CM-8, MP-4, RA-3, SC-7

Federal: FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AS-1, SM-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(A), 45 C.F.R. §164.308(a)(1)(ii)(B), 45 C.F.R. §164.308(a)(7)(ii)(E); NIST SP: 800-30, 800-39, 800-60; OMB Memo: M-07-16 Att. 1, A.2, M-06-16, M-14-04	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; security plan; security categorization documentation; and other relevant documents or records.
Interview: Organizational personnel with security categorization and risk assessment responsibilities.

RA-03: RISK ASSESSMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in the applicable security plan;
c. Reviews risk assessment results in accordance with the implementation requirements;
d. Disseminates risk assessment results to applicable senior agency officials (e.g., director or equivalent), affected stakeholders, Information Owner(s)/Custodian(s), and the HHS CISO; and
e. Updates the risk assessment according to the implementation requirements.

HIPAA:
The organization documents risk assessment results in a HIPAA Risk Analysis, and associated risks to PHI must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings. All HIPAA Risk Analysis documentation must be maintained for 6 years from the date of creation or date it was last in effect – whichever is later.

CMS-MARS-E:
c. The organization reviews risk assessment results within every three hundred sixty-five (365) days.
e. The organization updates the risk assessment every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system. (Significant change is defined in NIST Special Publication 800 37 Revision 1, Section F.4 of Appendix F.)

CONTROL IMPLEMENTATION STANDARDS

Std.1 - A Chief Information Security Officer will ensure a risk assessment of information resources is performed and documented by the information owners. The risk assessment (which is a self-assessment by the information owner) shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," "Moderate," or "Low." Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the state organization head or his or her designated representative(s).
Std.2 –Risk Assessment Frequency:
a. Initial System Risk Assessment: For new Information Systems, prior to moving into production, the Information Owner will complete a full review for compliance of all security and privacy controls required per the system categorization (see RA-2), documents the current implementation status of the controls in the system security plan (see PL-2), ensures required vulnerability scans are conducted (See RA-05), (and receive an authority to operate (ATO), per CA-6, prior to the system to moving to production.
b. Information Owner Annual Risk Assessment: The Information Owner, on an annual basis, will review the compliance status of all security and privacy controls required per the system categorization (see RA-2) of the information system, ensures required vulnerability scans are conducted (See RA-05), and documents the current implementation status of the controls in the system security plan (see PL-2).

c. Major System Change Risk Assessment: The Information Owner, when significant changes are made to the system or environment of operation (including identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system, will complete a full review for compliance of all impacted security and privacy controls required per the system categorization (see RA-2), documents the current implementation status of the controls in the system security plan (see PL-2), ensures required vulnerability scans are conducted (See RA-05), and receive a new security authorization in accordance with CA-6 prior to moving the significant changes into production.
Std.3 – Information Owners, or their delegate, will document system's non-compliance with required security and privacy controls that is identified during risk assessments per Information Security guidance and develop plans of actions or milestones (POA&M) to remediate the non-compliance in accordance with CA-5. Any risk acceptance for non-compliant security and privacy controls will be in accordance with CA-6 and TAC 202.25.

CMS-MARS-E:
Std.4 - The organization conducts an information risk assessment and documents risk assessment results in the security assessment report template that can be found at:
https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/
Std.5 - The system owner reviews risk assessment results at least every three hundred sixty-five (365) days or when a significant change occurs.

SUPPLEMENTAL GUIDANCE

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.
Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.

PHI:
The Department of Health and Human Services has issued Final Guidance on Risk Analysis (Assessment) under the HIPAA Security Rule (see
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf).

PII:
A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.

A standardized risk assessment process should include a consideration of risks associated with the collection, maintenance, and use of sensitive information such as PII. An evaluation of risks associated with the potential impact of loss of the PII must be identified within the overall risk assessment. All risk assessment documentation must reflect these findings.

Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. An evaluation of privacy risk for an information system benefits an organization and the individuals whose PII are included by

enabling the organization to identify, evaluate, and manage the privacy risks for the information in that system. The content of the privacy risk assessment performed under this control should be addressed in concert with the privacy risk evaluation conducted through the internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing privacy-related sensitive information.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** TAC 202.21(b)(6); TAC 202.24(a)(1); TAC 202.25(1-3); DIR Security Control Standards Catalog **Federal:** OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39; Web: http://idmanagement.gov; IRS1075; CJIS 5.6	RA-2; PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; system security plan; risk assessment; and other relevant documents or records. Interview: Organizational personnel with risk assessment responsibilities.	

RA-05: VULNERABILITY SCANNING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Scans for vulnerabilities in the information system and hosted applications at minimum of monthly for moderate and high systems and annually for low and low plus systems or as required by regulations and agreements, and when new vulnerabilities potentially affecting the components are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities based on the HHS defined risk prioritization in accordance with an organizational assessment of risk; and; e. Shares information obtained from the vulnerability scanning process and security control assessments with designated security personnel and system administrators on a “need to know” basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). **CMS-ARS:** a. Scans for vulnerabilities in the information system and hosted applications no less often than once every 72 hours and when new vulnerabilities potentially affecting the system/applications are identified and reported; d. Remediates legitimate vulnerabilities based on the HHS defined risk prioritization in accordance with the guidance defined under security control SI-02; and Cloud: This control requirement replaces RA-05(a): a. Scans for vulnerabilities in the information system and hosted applications at least every 30 days and when new vulnerabilities potentially affecting the system/applications are identified and reported. **CMS-MARS-E:** a. The organization scans for vulnerabilities in the information system and hosted applications, operating system, web application, and database scans (as applicable) within every thirty (30) days and when new vulnerabilities potentially affecting the system/applications are identified and reported. d. The organization remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk.	

IRS:
The agency must:
a. Scan for vulnerabilities in the information system and hosted applications at a minimum of monthly for all systems and when new vulnerabilities potentially affecting the system/applications are identified and reported

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Vulnerability scans must be performed when new vulnerabilities, risks, or threats potentially affecting the system/applications are identified and reported or upon request from HHS.
Std.2 - Vulnerability scanning tools results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Vulnerability scan information sources include systems, appliances, devices, services, and applications (including databases); and
(c) HHS Information Security directed vulnerability scan information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.3 - As required by HHS, raw results from vulnerability scanning tools must be available in an unaltered format to HHS Information Security.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational monitoring status and security posture information.

CMS-ARS:
Cloud:
Std.5 - For cloud service providers, the organization scans for vulnerabilities in the information system and hosted applications as required under DHS Continuous Diagnostics and Mitigation and NIST Continuous Monitoring guidelines for CSPs; and operating system, web application, and database scans (as applicable); and when new vulnerabilities potentially affecting the system/applications are identified and reported.
Std.6 - For cloud service providers, the organization remediates legitimate high-risk vulnerabilities within ten (10) days and moderate risk vulnerabilities within thirty (30) days. Use of time periods that exceed CMS standards but are approved and accepted by the JAB must be authorized by the CISO.

CMS-MARS-E:
Std.5 - Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with organizational Information Security procedures.
Std.6 - Legitimate high-risk vulnerabilities are mitigated within thirty (30) days, and moderate risk vulnerabilities are mitigated within ninety (90) days.

SUPPLEMENTAL GUIDANCE

Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example:
(i) scanning for patch levels;
(ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and
(iii) scanning for improperly configured or incorrectly operating information flow control mechanisms.
Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS).

CMS-ARS:
The organization remediates legitimate high-risk vulnerabilities within ten (10) days and moderate risk vulnerabilities within thirty (30) days.

Penetration testing is covered under CA-08.

REFERENCES	RELATED CONTROLS

Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-5, SM-5; HSPD 7: F(19), G(24); NIST SP: 800-37, 800-39, 800-40, 800-70, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; Web: cwe.mitre.org, nvd.nist.gov; IRS1075; CJIS 5.6	CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; vulnerability scanning results; patch and vulnerability management records; and other relevant documents or records. Examine: Information system provides the capability to perform an on-demand custom vulnerability assessment. Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities. The assessment capability must support an on-demand (manually initiated) vulnerability scan with predefined or custom content.	

RA-05(01): UPDATE TOOL CAPABILITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities scanned.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. **CMS-ARS:** The assessment capability must support updates that include predefined or custom content (i.e., meet Continuous Diagnostics and Mitigation required formats and updating frequencies) and provide the capability to update assessment content.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: F(19), G(24) NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	SI-3, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; and other relevant documents or records. Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities. Test: Vulnerability scanning capability and associated scanning tools.	

RA-05(02): UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS
The HHS organization updates the information system vulnerabilities scanned prior to a new scan and when new vulnerabilities are identified and reported. **CMS-MARS-E:** a. The organization updates the information system vulnerabilities scanned within every thirty (30) days or when new vulnerabilities are identified and reported. **CMS-ARS:** The organization updates the database of known information system vulnerabilities to be used in the scanning process no less often than every 72 hours, immediately prior to a new scan, and when new vulnerabilities are identified and reported. FedRAMP Rev. 4 Baseline; HSPD 7: F(19), G(24) NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04 Cloud: For cloud service providers, this Standard replaces the requirement defined within RA-05(02). The organization updates the list of information system vulnerabilities scanned no less often than before each scan.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; HSPD 7: F(19), G(24) NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	SI-3, SI-5

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; and other relevant documents or records. Examine: Information system updates vulnerability scanning data as required.

RA-05(03): BREADTH / DEPTH OF COVERAGE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs vulnerability scanning procedures that can identify/demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-100; OMB Memo: M-16-04; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; and other relevant documents or records.

RA-05(04): DISCOVERABLE INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization determines what information about the information system is discoverable by adversaries, and subsequently takes appropriate corrective actions to limit discoverable system information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-37, 800-39, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	AU-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; and other relevant documents or records.	

RA-05(05): PRIVILEGED ACCESS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Automated scanning tool functionality must be compliant with HHS requirements to include the ability to perform credentialed scans. (a) To the extent possible, credentials will be compliant with HHS policy. Std.2 - Credentialed scanning must be performed on all information systems and network devices (including appliances). Std.3 - The organization must maintain and provide changes to the system accounts to support credentialed scanning no later than two (2) weeks prior to expiration or when other changes to the accounts are needed.	
SUPPLEMENTAL GUIDANCE	
In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning. **CMS-ARS:** Privileged access mechanisms must be compliant with HHS requirements for access to elevated privilege accounts. The assessment capability must support use of credentialed scans. Credentialed access is compliant with HHS policy.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.308(a)(1)(i), 45 C.F.R. §164.316(a); NIST SP: 800-12, 800-30, 800-37, 800-39, 800-100, 800-115, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: Risk assessment policy; procedures addressing vulnerability scanning; system security plan; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; and other relevant documents or records. Examine: Information system provides the capability to perform scans using appropriate credentials. Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities.

RA-05(06): AUTOMATED TREND ANALYSES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	IR-4, IR-5, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; vulnerability scanning results; and other relevant documents or records. Test: Vulnerability scanning capability and associated scanning tools.	

RA-05(08): REVIEW HISTORIC AUDIT LOGS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	AU-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Risk assessment policy; procedures addressing vulnerability scanning; audit logs; records of audit log reviews; vulnerability scanning results; patch and vulnerability management records; and other relevant documents or records. Interview: Organizational personnel with risk assessment and vulnerability scanning responsibilities; system/network administrators; and organizational personnel with information security responsibilities. Test: Organizational processes for vulnerability scanning; organizational process for audit record review and response; automated mechanisms/tools supporting and/or implementing vulnerability scanning; and automated mechanisms supporting and/or implementing audit record review.	

(SA) SYSTEM AND SERVICES ACQUISITION

The HHS organization (i) requires sufficient allocation of resources to adequately protect HHS information systems; (ii) employs system development life cycle processes that incorporate information security considerations; (iii) employs software usage and installation restrictions; and (iv) requires that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from HHS.

SA-01: SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates (as necessary) the current: 1. System and services acquisition policy within every three (3) years; and 2. System and services acquisition procedures within every three hundred and sixty five (365) days. **CMS-MARS-E:** b.1. System and services acquisition policy within every three hundred and sixty five (365) days	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-100; IRS1075	PM-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy and procedures; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities.	

SA-02: ALLOCATION OF RESOURCES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The organization:
a. Determines information security requirements for the information systems in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the HHS information systems or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation

CMS-MARS-E/CMS-ARS:
d. The organization includes information security requirements in mission/business case planning.

CMS-ARS:
PII:
As part of the capital planning and investment control process, the organization must determine, document, and allocate resources required to protect the privacy and confidentiality of personally identifiable information (PII) in the information system.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The agency head or his/her designated representative(s) shall allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the agency head.
Std.2 - The state organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

SUPPLEMENTAL GUIDANCE

Resource allocation for information security includes funding for the initial information system or information system service acquisition and funding for the sustainment of the system/service.

PII:
Resources must be considered for the protection of privacy and confidentiality when budgeting for an information system.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** TAC 202.20(2); DIR Security Control Standards Catalog **Federal:** E-Government Act of 2002 (Pub. L. No. 107-347), §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-1, AS-3, CM-3, SM-1; NIST SP: 800-65; OMB Memo: M-16-04; OMB Circular A-130: 7.g. and 8.b(3)(b); IRS1075; CJIS 5.6	PM-3, PM-11

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; organizational programming and budgeting documentation; other relevant documents or records.
Interview: Organizational personnel with capital planning and investment responsibilities.

SA-03: SYSTEM DEVELOPMENT LIFE CYCLE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Manages the information system using a formally defined and documented System Development Life cycle (SDLC) process that incorporates information security considerations
b. Defines and documents information security roles and responsibilities throughout the system development life cycle;
c. Identifies individuals having information system security roles and responsibilities; and

d. Integrates the HHS organizational information security risk management process into system development life cycle activities.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The agency head shall ensure that information security management processes are integrated with agency strategic and operational planning processes.
Std.2 - The Chief Information Security Officer (CISO) is responsible for:
a. Working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of TAC 202 and the agency's information security risk.
b. Development and recommending procedures and practices, in cooperation with the agency Information Resources Manager; information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure.
Std.3 - Information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process.
Std.4 - The Information Owner or his or her designated representative(s) are responsible for:
a. Formally assigning custody of information or an information resource
b. Coordinating data security control requirements with the ISO
c. Conveying data security control requirements to custodians
d. Providing authority to custodians to implement security controls and procedures
e. Justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the agency information security officer.
f. Participating in risk assessments as provided under §202.25 of this chapter.
Std.5. - Custodians of information resources, including third party entities providing outsourced information resources services shall:
a. Implement controls required to protect information and information resources required by TAC 202 based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the agency information security program.
b. Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.
c. Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents.
d. Provide information necessary to provide appropriate information security training to employees.
e. Ensure information is recoverable in accordance with risk management decisions.
Std.6 - HHS shall review its requirements for forms, data collection, and notarization when planning to deliver a service through the Internet to determine if the information is necessary and, if necessary, the appropriate level of authentication. Based on this review, the agency shall:
a. eliminate any unnecessary requirements; and
b. adjust security to the appropriate level for any necessary requirements.

CMS-ARS:
Std.6 - The information system must be managed using:
(a) The information security steps of IEEE 12207.0 standard for SDLC, as defined in the CMS eXpedited Life Cycle (XLC), to incorporate information security control considerations; and
(b) The information system architecture defined within the Technical Reference Architecture (TRA).

SUPPLEMENTAL GUIDANCE

A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To
apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business

processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies.

PII:
To ensure that privacy and security controls are appropriately considered during each phase of the SDLC, both the security and privacy offices should have a clear understanding of the requirements to protect PII. The privacy office should participate throughout the SDLC.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** TAC 202.20(8); TAC 202.21(b)(3); TAC 202.21(b)(8); TAC 202.22(1-2); TGC 2054.112; DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-37, 800-64; OMB Circular A-130; IRS1075	AT-3, PM-7, SA-8

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; information system development life cycle documentation; other relevant documents or records.
Interview: Organizational personnel with information security and system life cycle development responsibilities.

SA-04: ACQUISITION PROCESS

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

PII:
When acquiring information systems, components, or services used to store, process, or transmit personally identifiable information (PII), ensure the following, in consultation with the privacy office, are included in the acquisition contract:
h. List of security and privacy controls from the Privacy Overlays necessary to ensure protection of PII and, if appropriate, enforce applicable privacy requirements.
i. Privacy requirements set forth in Appendix J of NIST SP 800-53, Rev. 4, including privacy training and awareness, and rules of behavior.
j. Privacy functional requirements, i.e., functional requirements specific to privacy.
k. Federal Acquisition Regulation (FAR) Clauses per FAR Part 24 and Part 39.105, and any other organization specific privacy clause

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The state organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws and standards.
Std.2 - The Chief Information Security Officer (CISO) is responsible to:

a. Coordinate the review of data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data.
b. Verify that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data.

HIPAA:
Std.3 - When acquiring information systems, components, or services used to store, process, or transmit PHI, in addition to the requirements for PII, ensure the following in consultation with the privacy office:
1. Necessary memorandum of understanding, memorandum of agreement, or other data sharing agreement are obtained.

CMS-MARS-E:
Std.4 - Each contract and Statement of Work (SOW) that requires development or access to systems that contain Personally Identifiable Information (PII) must include language requiring adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR §155.260(b); define security and privacy roles and responsibilities; and receive approval from the system owner.
Std.5. When contracting with external service providers,
a. as part of the service contract, the AE must establish security and privacy policies and procedures for how data is stored, handled, and accessed within service provider environment.
b. the data must be encrypted in transit to and from the service provider environment.
c. all mechanisms used to encrypt data must be FIPS 140-2 validated, and operate using the FIPS 140-2 validated module.
d. storage devices where data has resided must be securely sanitized according to MARS-E MP-6 Media Sanitization security control prior to use.
e. per SA-9(5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS.

SUPPLEMENTAL GUIDANCE

Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: Development processes, procedures, practices, and methodologies; and Evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle.

Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services.

Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA.

PII:
Contracts for information systems, components, or services must meet the privacy requirements of the federal government and it is much easier, and cheaper, to build privacy into a system at the acquisition phase of the life cycle than it is to bolt it on after the system is already acquired.

REFERENCES	RELATED CONTROLS

Texas HHS: IS-Policy **State:** TAC 202.21(b)(9); TAC 202.21(b)(10) **Federal:** 5 U.S.C. §552a(m) and (e)(10); E-Government Act of 2002: (I; Pub. L. No. 107-347) §208; FAR: Part 24 and 39.105; Federal Information Management Security Act (Pub. L. No. 107-347); FedRAMP Rev. 4 Baseline; FIPS Pub: 140-2; FISCAM: AS-3, CM-3; HIPAA: 164.314(a)(2 (i); NIST SP: 800-23, 800-35, 800-36, 800- 37, 800-64, 800-70, 800-137; OMB Memo: M-16-04; OMB Circular A-130: 7.g. and Appendix 1; Web: acquisition.gov/far, fips201ep.cio.gov, niap-ccevs.org; 45 C.F.R. §164.314(a); IRS1075; CJIS 5.6	CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12, AR-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts for information systems or services; other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.	

SA-04(01): FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	SA-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.	

SA-04(02): DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: a. Security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces; b. High-level design documentation at sufficient detail to prove the security control implementation.	

CMS-ARS: c. Source code and hardware schematics.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	SA-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records.	

SA-04(08): CONTINUOUS MONITORING PLAN

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that meets CMS and Federal requirements (e.g., Continuous Diagnostics and Mitigation, ongoing authorization).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	CA-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing developer continuous monitoring plans; procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process; developer continuous monitoring plans; security assessment plans; acquisition contracts for the information system, system component, or information system service; acquisition documentation; solicitation documentation; service-level agreements; and other relevant documents or records. Interview: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with responsibility for determining information system security requirements; information system developers; organizational personnel with information security responsibilities.	

SA-04(09): FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; OMB Memo: M-16-04; CJIS 5.6	CM-7, SA-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.	

SA-04(10): USE OF APPROVED PIV PRODUCTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, VA
CONTROL REQUIREMENTS	
The organization employs only information technology products on the FIPS 201-approved products list for PIV capability implemented within organizational information systems.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	IA-2, IA-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.	

SA-05: INFORMATION SYSTEM DOCUMENTATION

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Obtains administrator documentation for the information system, system component, or information system service that describes:
1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security functions/mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent, and evaluate whether such documentation is essential for the effective implementation or operation of security controls;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to defined personnel or roles (defined in the applicable system security plan [SSP]).

CONTROL IMPLEMENTATION STANDARDS

CMS-MARS-E:
Std.1 - The organization:
a. Develops system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users.
b. Maintains an updated list of related system operations and security documentation.
c. Updates documentation upon changes in system functions and processes.
d. Must include date and version number on all formal system documentation.

SUPPLEMENTAL GUIDANCE

This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, AS-5, CM-2, CP-2; OMB Memo: M-16-04; IRS1075; CJIS 5.6	CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent information system documentation; other relevant documents or records. Interview: Organizational personnel with information system documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system.

SA-08: SECURITY ENGINEERING PRINCIPLES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. **IRS:** The agency must apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system. Security engineering principles include, for example: 1. developing layered protections 2. establishing sound security policy, architecture, and controls as the foundation for design 3. incorporating security requirements into the system development lifecycle 4. delineating physical and logical security boundaries 5. ensuring that system developers are trained on how to build secure software 6. tailoring security controls to meet organizational and operational needs 7. performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk 8. reducing risk to acceptable levels, thus enabling informed risk management decisions.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - The information system must follow system security engineering principles consistent with: (a) The information security steps of the HHS eXpedited Life Cycle (XLC) to incorporate information security control considerations; (b) The information system architecture defined within the Technical Reference Architecture (TRA); and (c) The Technical Review Board (TRB) processes defined by HHS.	
SUPPLEMENTAL GUIDANCE	
Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) Developing layered protections; (ii) Establishing sound security policy, architecture, and controls as the foundation for design; (iii) Incorporating security requirements into the system development life cycle; (iv) Delineating physical and logical security boundaries; (v) Ensuring that system developers are trained on how to build secure software; (vi) Tailoring security controls to meet organizational and operational needs; (vii) Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) Reducing risk to acceptable levels, thus enabling informed risk management decisions. PII: When applying information system security engineering principles in the specification, design, development, implementation, and modification of an information system containing personally identifiable information (PII), the organization should apply privacy-enhanced system design and development principles described in NIST SP 800-53, Rev. 4, Appendix J.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	PM-7, SA-3, SA-4, SA-17, SC-2, SC-3, AR-7

Federal: E-Government Act of 2002 (Pub. L. 107-347) §208; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-27; OMB Memo: M-16-04, M-05-08, M-03-22; OMB Circular A-130: 7.g.; IRS1075	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records.
Interview: Organizational personnel with information system design, development, implementation, and modification responsibilities.

SA-09: EXTERNAL INFORMATION SYSTEM SERVICES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Requires that providers of external information system services comply with HHS organizational information security requirements and employ appropriate controls in accordance with applicable state laws, federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services in a SLA or similar agreement; and
c. Employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.

CMS-MARS-E:
d. The organization must notify CMS of plans to outsource information system services prior to the awarding of contract. Per SA-9(5), the outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS.
e. The organization ensures that service level agreements define expectations of performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

CONTROL IMPLEMENTATION STANDARDS

HIPAA:
Std.1 - A covered entity or business associate under HIPAA or HITECH may create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations.

IRS:
Std.1 - The contract for the acquisition must contain Exhibit 7 language, as appropriate (see Section 9.3.15.4, Acquisition Process (SA-4), and Exhibit 7, Safeguarding Contract Language
Std.2 - Agencies must prohibit the use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI unless explicitly approved by the Office of Safeguards. For notification requirements, refer to Section 7.4.5, Non-Agency-Owned Information Systems.

CMS-MARS-E:
Std.1 - The service contract or agreement must include language requiring:
a. The provider to be subject to U.S. Federal laws and regulations protecting PII.
b. Adherence to the security and privacy policies and standards set by the organization consistent with 45 CFR 155.260(b), define security and privacy roles and responsibilities.
Std.2 The AE must notify CMS at least 45 days prior to transmitting data into an external information service environment.

SUPPLEMENTAL GUIDANCE

External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance.

PHI:
The information security requirements and controls are documented through a written contract, or other arrangement that meets the requirements of 45 C.F.R. §164.314(a). This guidance is not intended to cover the acquisition of services of all third party providers, only those who rise to the level of a business associate of a covered entity.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; HIPAA: 45 C.F.R. §164.530; 45 C.F.R. §164.308(b)(1), 45 C.F.R. §164.308(b)(4), 45 C.F.R. §164.314(a)(1), 45 C.F.R. §164.314(a)(2)(i), 45 C.F.R. §164.314(a)(2)(ii); Homeland Security Presidential Directive (HSPD) 7: D(8); NIST SP: 800-35; OMB Memo: M-16-04; IRS1075; CJIS 5.6	CA-3, IR-7, PS-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; and other relevant documents or records.
Examine: Organization facilitates required oversight of privacy reporting by CMS (to include coordination and cooperation with the CMS Cybersecurity Integration Center [HHS Information Security]).
Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

SA-09(01): RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization:
a. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services;

CMS-ARS:
b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by Joint Authorization Board (JAB).

CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - The organization documents all existing outsourced information services and conducts a risk assessment of future outsourced information services. **CMS-ARS:** Std.1 - For CSPs, the organization documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are approved and accepted by the JAB.	
SUPPLEMENTAL GUIDANCE	
Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	CA-6, RA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; (ii) The organization defines the senior organizational official designated to approve the acquisition or outsourcing of dedicated information security services; (iii) The designated senior organizational official approves the acquisition or outsourcing of dedicated information security services; and (iv) The organization meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; risk assessment reports; and other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities. **HIPAA:** Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.	

SA-09(02): IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires providers of external information system services, as defined in the applicable System Security Plan, to identify the functions, ports, protocols, and other services required for the use of such services.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	CM-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security	

specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

SA-09(04): CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
CSP: The organization employs security safeguards (defined in the system security plan [SSP]) to ensure that the interests of external service providers are consistent with and reflect organizational interests.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts for the information system, system component, or information system service; solicitation documentation; acquisition documentation; service-level agreements; organizational security requirements/safeguards for external service providers; personnel security policies for external service providers; assessments performed on external service providers; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; external providers of information system services. Test: Organizational processes for defining and employing safeguards to ensure consistent interests with external service providers; automated mechanisms supporting and/or implementing safeguards to ensure consistent interests with external service providers.	

SA-09(05): PROCESSING, STORAGE, AND SERVICE LOCATION

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, CMS-ARS, IRS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization restricts the location of information processing, information/data system services to the Continental United States unless implementation standard 1 is met. **CMS-ARS:** PII: If the service provider will be maintaining personally identifiable information (PII) outside of the United States, the organization must evaluate the legal environment of the country in which the information will be maintained to ensure US equities are protected. If the service provider is located in the US and the PII is about non-US Citizens, then the organization must address the data transfer requirements of the country whose citizens PII is collected or maintained and must ensure that country's privacy/data protection legal requirements are met. Coordinate with your organization's legal counsel, privacy office, and Department of State representative in meeting this requirement. Cloud The organization restricts the location of information processing, information/data, and information system services to organization-defined locations based on program requirements or conditions. In no case may the safeguards afforded to sensitive information be less than the safeguards mandates by CMS, federal law, Executive Order, or other authoritative direction.	

CMS-MARS-E: a. The outsourcing of information system services outside the continental U.S. must be authorized by the CIO of CMS. b. Depending on the outcome of the risk assessment, the organization may need to restrict the location of information systems that receive, process, store, or transmit PII to areas within United States territories, embassies, or military installations.
CONTROL IMPLEMENTATION STANDARDS
Std.1 - The applicant/bidder ensures that services which access, create, disclose, receive, transmit, maintain, or store HHS Confidential Information are maintain in the United States (no offshoring) unless all of the following requirements are met: a. The data is encrypted with FIPS 140-2 compliant encryption b. The offshore provider does not have access to the encryption keys c. The applicant/bidder maintains the encryption key within the United States d. The applicant/bidder has obtained the express prior written permission of the HHS agency **IRS:** Std.1 - Restrict the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations.
SUPPLEMENTAL GUIDANCE
Other countries have different requirements for the protection of PII of either their own citizens or for transfer of PII across national borders. When selecting a service provider, the location for storage, maintenance, or processing must be considered. Some organizations, such as European Union member states, have very stringent data transfer restriction requirements and your organization may have a treaty or other agreement for data exchange and/or protection. Consult with your legal counsel or your organization's liaison to the Department of State.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; OMB Circular A-130: 7.g., 9.b and 9.c.	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services.

SA-10: DEVELOPER CONFIGURATION MANAGEMENT

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service development, implementation, and operation; b. Document, manage, and control the integrity of changes to configuration items under configuration management; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable system security plan [SSP]).	
CONTROL IMPLEMENTATION STANDARDS	

Std.1 - All security-related information resources changes shall be approved by the information owner through a change control process. Approval shall occur prior to implementation by the state organization or independent contractors. **SPI:** Std.2 - The applicant/bidder implements computer security configurations or settings for all computers and systems that access or store HHS Confidential Information? (e.g., non-essential features or services have been removed or disabled to reduce the threat of breach and to limit exploitation opportunities for hackers or intruders, etc.)
SUPPLEMENTAL GUIDANCE
This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; NIST SP: 800-128; OMB Memo: M-16-04; IRS1075; CJIS 5.6	CM-3, CM-4, CM-9, SA-12, SI-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records. Interview: Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities.

SA-10(01): SOFTWARE / FIRMWARE INTEGRITY VERIFICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline	SI-7, AP-1, AP-2, UL-02

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records. Interview: Organization personnel with information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities.

SA-11: DEVELOPER SECURITY TESTING AND EVALUATION

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan in accordance with, but not limited to, current HHS procedures; b. Perform (one or more) unit, integration, system, regression testing/evaluation in accordance with the current HHS procedures; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation. **CMS-ARS:** For information systems containing PII, the organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan that includes assessment of privacy controls. b. In testing: 1. Minimize to the use of PII to the maximum extent practicable; 2. Only conduct testing with actual PII if a formal memorandum of agreement (MOA), memorandum of understanding (MOU), or data exchange agreement has been established between the data owner of the PII and the entity developing/testing the information system including how loss, theft, or compromise (i.e., breach) of PII is to be handled; 3. Receive formal approval for the use of PII with the privacy office before conducting any testing, and PII must be de-identified or anonymized to the maximum extent practicable.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate, High: Std.1 - Agency will submit a biennial data security plan to the Department of Information Resources (DIR) no later than October 15 of each even-numbered year to establish planned beta testing for websites or applications that process any sensitive personal information or confidential information. **Web & Mobile:** Std.2 - Regularly review code looking for common issues like SQL Injection and Cross-Site Scripting. Std.3 - Conduct security testing both during and after development to ensure the application meets security standards. Std.4 - Third Party code libraries should be reviewed for bugs and security vulnerabilities before being included into a web application. Std.5 - External web based services used in the web application should be evaluated for security before use (e.g. Geolocation, Calendar, or Email services). **CMS-ARS, CMS-MARS-E:** Std.6 - If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. Std.7 - Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.	

Std.8 - All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network Technical Reference Architecture traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists (ACLs) as well as ports and protocols.
SUPPLEMENTAL GUIDANCE
Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. PII: Testing is a key method to ensure privacy controls are implemented. Including privacy controls in the security assessment plan ensures they are tested.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** TGC 2054.516; DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. No. 107-347), §208, and Title III; FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-3; ISO/IEC: 15408; OMB Memo: M-03-22; OMB Circular A-130: 7.g.; Web: capec.mitre.org, cve.mitre.org, cwe.mitre.org, nvd.nist.gov; IRS1075; CJIS 5.6	CA-2, CM-4, SA-3, SA-4, SA-5, SI-2, AR-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.

SA-11(01): STATIC CODE ANALYSIS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): Web & Mobile, CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile:	

Std. 1 - Systems with Internet website or mobile applications that process any sensitive personal information or confidential information must subject the website or mobile application to a vulnerability test and address any vulnerabilities identified in the test.

CMS-ARS:
Cloud
Std.2 - For cloud service providers, the organization submits a code analysis report as part of the authorization package and update the report in any reauthorization actions.
Std.3 - For Cloud Service Providers, the organization documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

CMS-MARS-E:
Std.2 - The organization submits a code analysis report as part of the authorization package and update the report in any reauthorization actions.
Std.3 - The organization documents in the Continuous Monitoring Plan how newly developed code for the information system is reviewed.

SUPPLEMENTAL GUIDANCE

Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Web and Mobile Minimum Security Standard **State:** TGC 2054.516 **Federal:** FedRAMP Rev. 4 Baseline	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis; and
(ii) The organization meets all the requirements specified in the applicable Implementation Standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; and other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

SA-11(02): THREAT AND VULNERABILITY ANALYSIS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

CONTROL IMPLEMENTATION STANDARDS

Web & Mobile:
Std. 1 - Systems with Internet website or mobile applications that process any sensitive personal information or confidential information must subject the website or mobile application to a vulnerability test and address any vulnerabilities identified in the test.

SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Web and Mobile Minimum Security Standard **State:** TGC 2054.516 **Federal:** FedRAMP Rev. 4 Baseline	PM-15, RA-5

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator threat and vulnerability analyses; information system developer/integrator threat and vulnerability test plans; records of developer/integrator threat and vulnerability testing results for the information system; threat and vulnerability flaw tracking records; other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.

SA-11(05): PENETRATION TESTING

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): Web & Mobile, CMS-ARS
CONTROL REQUIREMENTS	
The organization requires information systems, system components, and information system services to undergo penetration testing prior to deployment in the production environment, in a manner that is no less stringent than required under CA-8.	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std.1 - This control only applies to systems with Internet accessible website or mobile applications that process any sensitive personal information or confidential information Std.2 - Systems with Internet accessible website or mobile applications that process any sensitive personal information or confidential information must subject the website or mobile application to a penetration test and address any vulnerabilities identified in the test.	
SUPPLEMENTAL GUIDANCE	
Provides for implementation of penetration testing as identified in CA-8.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Web and Mobile Minimum Security Standard **State:** TGC 2054.516 **Federal:** Code: 5 U.S.C. §552a(b) and (e)(10); NIST SP: 800-115; GAO; OMB Circular A-130: 7.g. and 8.b.(2)(c)(iii)	CA-8

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; and other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities. Test: Organizational processes for monitoring developer security testing and evaluation; automated mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation.

SA-11(08): DYNAMIC CODE ANALYSIS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): Web & Mobile, CMS-ARS
CONTROL REQUIREMENTS	
The organization requires information systems, system components, and information system services to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std. 1 - Systems with Internet website or mobile applications that process any sensitive personal information or confidential information must subject the website or mobile application to a vulnerability test and address any vulnerabilities identified in the test.	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Web and Mobile Minimum Security Standard **State:** TGC 2054.516 **Federal:** FedRAMP Rev. 4 Baseline; OMB Memo: M-14-03, M-15-01, M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; and other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.	

SA-12: SUPPLY CHAIN PROTECTION

Priority: P1	
Baseline(s): High	Overlay(s): DIR, CMS-ARS
CONTROL REQUIREMENTS	
The organization protects against supply chain threats to the information system, system component, or information system service by employing best practices and methodologies; and wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security strategy.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control enhancement also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation	

are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** NIST IR: 7622; NIST SP: 800-161; OMB Memo: M-16-04	AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; information system development life cycle documentation; other relevant documents or records.	

SA-12(02): SUPPLIER REVIEWS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; records of supplier due diligence reviews; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities. Test: Organizational processes for conducting supplier reviews; automated mechanisms supporting and/or implementing supplier reviews.	

SA-13: TRUSTWORTHINESS

Priority: P2	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization:	

a. Describes (in the applicable system security plan [SSP]) the trustworthiness required in information systems, information system components, or information system services
supporting its essential missions/business functions; and
b. Implements a level of security-functionality and security-assurance that is sufficient to preserve the confidentiality, integrity, and availability of the information being processed,
The organization:
a. Describes (in the applicable system security plan [SSP]) the trustworthiness required in information systems, information system components, or information system services supporting its essential missions/business functions; and
b. Implements a level of security-functionality and security-assurance that is sufficient to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system, by following the CMS eXpedited Life Cycle (XLC) and the system authorization process.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). Developers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in NIST 800-53
Appendix E).

Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in NIST 800-53 Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in NIST 800-53 Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, government wide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems.

REFERENCES	RELATED CONTROLS
Federal: FIPS Pub: 199, 200; NIST SP: 800-60, 800-64; OMB Memo: M-16-04	RA-2, SA-4, SA-8, SA-14, SC-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; information system design documentation; security requirements and security specifications for the information system; penetration test and vulnerability scan reports; security test and evaluation results; authority to operate documentation; other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities; information system authorizing official.

SA-14: CRITICALITY ANALYSIS

Priority: P2	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The organization identifies critical information system components and functions by performing a criticality analysis for organization information systems, information system components, or information system services at organization-defined decision points in the system development life cycle.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades.	
REFERENCES	**RELATED CONTROLS**
Federal: HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)	CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing criticality analysis requirements for information systems, security plan; contingency plan; list of information systems, information system components, or information system services requiring criticality analyses; list of critical information system components and functions identified by criticality analyses; criticality analysis documentation; business impact analysis documentation; system development life cycle documentation; other relevant documents or records. Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibilities for performing criticality analysis for the information system.	

SA-15: DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Priority: P2	
Baseline(s): High	Overlay(s): DIR, CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations at least every three (3) years to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Development tools include, for example, programming languages and computer-aided design systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** OMB Memo: M-16-04	SA-3, SA-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.	

SA-15(09): USE OF LIVE DATA

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization disallows use of live data in development and test environments for the information system, system component, or information system service without prior approval of the Authorizing Official (AO). If approved by the AO, the organization documents and controls the use of live data in the development and test environments for the information system, system component, or information system service at a level commensurate with the sensitivity of the data and in a manner that minimizes the use of live data. Before use of live data containing personally identifiable information (PII) in a preproduction environment, the organization must: a. Implement policies and procedures in coordination with the privacy office for evaluating the risk of use of PII in a preproduction environment; b. Protect, per NIST SP 800-122, the PII within the preproduction environment at the same level as in the production environment; and c. Use anonymized data substitution (See NIST SP 800-122, Section 4.2.4) if possible.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Preproduction environments may not be as formally controlled as production environments. Use of sensitive information, including PII, in a preproduction environment increases risk to the organization, because the preproduction environment may not be as secure as the production environment. If PII will be provided to a third-party during testing, the organization will need a formal MOA, MOU, or data exchange agreement before providing access to that third-party. Such agreement will at a minimum include how loss, theft, or compromise of PII is to be handled.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(b) and (e)(10); NIST SP 800-122	SA-9, DM-1(1), DM-3, UL-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the PII control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service-level agreements; acquisition contracts for the information system, system component, or information system service; information system design documentation; information system configuration settings and associated documentation; documentation authorizing use of live data in development and test environments; and other relevant documents or records.	

Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; system developer. Test: Organizational processes for approving, documenting, and controlling the use of live data in development and test environments; automated mechanisms supporting and/or implementing the approval, documentation, and control of the use of live data in development and test environments.

SA-16: DEVELOPER-PROVIDED TRAINING

Priority: P2	
Baseline(s): High	Overlay(s): DIR, CMS-ARS
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials), for affected personnel, on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog	AT-2, AT-3, SA-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.	

SA-17: DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS
CONTROL REQUIREMENTS	
The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture (see PL-8), which is established within and is an integrated part of the organization's enterprise architecture (see PM-7); b. Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. **CMS-ARS:** d. PII: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that accurately and completely describes the privacy requirements and the allocation of security and privacy controls among physical and logical components	
CONTROL IMPLEMENTATION STANDARDS	

SUPPLEMENTAL GUIDANCE
This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture, and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. PII: The security architecture and design identifies security and privacy controls necessary to support privacy requirements. The CMS Senior Official for Privacy is the best resource for identifying privacy requirements and privacy controls.

REFERENCES	RELATED CONTROLS
State: DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(10); E-Government Act of 2002 (Pub. L. No. 107-347) Title III; OMB Memo: M-05-08	PL-8, PM-7, SA-3, SA-8, AR-7

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; security flaw tracking records; other relevant documents or records. Interview: Organizational personnel with developer security testing responsibilities.

SA-21: DEVELOPER SCREENING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization requires that the developer of information systems, system components, or information system services: a. Have appropriate access authorizations as determined by assigned duties; and b. Satisfy personnel screening criteria as defined by HHS. PII: The organization requires that the developer of systems containing personally identifiable information (PII): a. Have appropriate access authorizations as determined by the assigned contracting officer and contracting officer representative, in consultation with the organization's privacy office; and b. Satisfy organization defined personnel screening criteria commensurate with increasing level of risk and responsibility for access to, or use of, different levels of PII.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
PHI: Under HIPAA, this is an addressable control. PII: Access to sensitive information, such as PII and protected health information (PHI), requires both a valid need to know as documented by an access authorization request and requires a background investigation (or appropriate screening) to ensure the individual being provided access is suitable. These access authorization requirements extend to developers of information systems containing sensitive information.	
REFERENCES	**RELATED CONTROLS**

Federal: Code: 5 C.F.R. §731.106; OMB Memo: M-16-04; 45 C.F.R. §164.308(a)(3)(ii)(B)	PS-3, PS-7, AR-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

PII:
Determine if the organization:
(i) Defines the information system, system component, or information system service for which the developer is to be screened;
(ii) Defines official government duties to be used to determine appropriate access authorizations for the developer;
(iii) Defines additional personnel screening criteria to be satisfied by the developer; and
(iv) Requires that the developer of organization-defined information system, system component, or information system service have appropriate access authorizations as
determined by assigned organization-defined official government duties; and
(v) Requires that the developer of organization-defined information system, system component, or information system service satisfy organization-defined additional personnel screening criteria.

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing information system developer/integrator access authorization; procedures addressing information system developer/integrator personnel screening; CMS personnel screening criteria; acquisition contracts and service level agreements; other relevant documents or records.
Interview: Organizational personnel with developer security testing responsibilities.

PII:
Examine: System and services acquisition policy; personnel security policy and procedures; procedures addressing personnel screening; information system design documentation; information system configuration settings and associated documentation; list of appropriate access authorizations required by developers of the information system; personnel screening criteria and associated documentation; and other relevant documents or records.
Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for developer screening.
Test: Organizational processes for developer screening; automated mechanisms supporting developer screening.

SA-22: UNSUPPORTED SYSTEM COMPONENTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization:
a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and
b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

IRS:
a. The agency must replace information system components (specifically security patches and/or product updates) when support for the components is no longer available from the developer, vendor, or manufacturer.
c. During a Safeguards on-site review, any unsupported system that is identified will not be tested and will result in a critical finding.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FISCAM: AS-3, CM-2; HHS: End of Life Operating Systems and Applications Policy; NIST SP: 800-70, 800-128; OMB Memo: M-07-11, M-	PL-2, SA-3

07-18, M-08-22, M-16-04; Web: checklists.nist.gov, nsa.gov, nvd.nist.gov; IRS1075	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and services acquisition policy; procedures addressing replacement or continued use of unsupported information system components; documented evidence of replacing unsupported information system components; documented approvals (including justification) for continued use of unsupported information system components; and other relevant documents or records.
Examine: Information system, devices, appliances and applications for versions that are no longer supported.
Interview: Organizational personnel with system and services acquisition responsibilities; organizational personnel responsible for configuration management.
Test: Automated mechanisms supporting and/or implementing replacement of unsupported system components.

(SC) SYSTEM AND COMMUNICATIONS PROTECTION

The HHS organization (i) requires the monitoring, control, and protection of HHS communications (information transmitted or received by HHS information systems) at the external and key internal boundaries of the information systems; and (ii) employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within HHS information systems.

SC-01: SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities,
and compliance; and
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
b. Reviews and updates (as necessary) the current:
1. System and communications protection policy within every three (3) years; and
2. System and communications protection procedures within every three hundred and sixty five (365) days.

CMS-MARS-E:
b.1. System and communications protection policy within every three hundred and sixty five (365) days.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	PM-9

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; NIST SP: 800-12, 800-100; IRS1075	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy and procedures; system security plan; and other relevant documents or records.
Interview: Organizational personnel with system and communications protection responsibilities. Verify personnel:
1. Know of system and communications protection policy and procedures; and
2. Are responsible for reviewing and updating system and communications protection policy and procedures no less often than required.

SC-02: APPLICATION PARTITIONING

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system separates user functionality (including user interface services) from information system management functionality.

CMS-ARS:
PII: In any situation where personally identifiable information (PII) is present, PII must be stored on a logical or physical partition separate from the applications and software partition.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, and servers and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical. Organizations implement separation of system management-related functionality from user functionality by using different computers, different central processing units, different instances of operating systems, different network addresses, virtualization techniques, or combinations of these or other methods, as appropriate. This type of separation includes, for example, web administrative interfaces that use separate authentication methods for users of any other information system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

It is necessary to store sensitive information, such as PII, on separate logical partitions from applications and software that provide user functionality to restrict accidental or unintentional loss of, or access to, sensitive information by both unauthorized users and unauthorized applications.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; 5 U.S.C. §552a(e)(10); OMB Circular A-130, 7.g. and 8.b.(3); 45 C.F.R. §164.312(a)(1); IRS1075; CJIS 5.6	SA-4, SA-8, SC-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Test: Separation of user functionality from information system management functionality.

SC-2(01): INTERFACES FOR NON-PRIVILEGED USERS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system prevents the presentation of information system management-related functionality at an interface for non-privileged users.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement ensures that administration options (e.g., administrator privileges) are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). Such restrictions include, for example, not presenting administration options until users establish sessions with administrator privileges.	
REFERENCES	**RELATED CONTROLS**
	AC-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; non-privileged users of the information system; system developer. Test: Separation of user functionality from information system management functionality.	

SC-03: SECURITY FUNCTION ISOLATION

Priority: P1	
Baseline(s): High	Overlay(s): DIR, CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system isolates security functions from non-security functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The information system isolates security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. Information systems implement code separation (i.e., separation of security functions from non-security functions) in a number of ways, including, for example, through the provision of security kernels via processor rings or processor modes. For non-kernel code, security function isolation is often achieved through file system protections that serve to protect the code on disk and address space protections that protect executing code. Information systems restrict access to security functions through the use of access control mechanisms and by implementing least privilege capabilities. While the ideal is for all of the code within the security function isolation boundary to only contain security-relevant code, it is sometimes necessary to include non-security functions within the isolation boundary as an exception.	
REFERENCES	**RELATED CONTROLS**
State: DIR Security Control Standards Catalog **Federal:** FISCAM: AC-4, AS-2; CJIS 5.6	AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	

ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems separate the security functions of the information system from non-security functions. Test: Separation of security functions from non-security functions within the information system.

SC-03(02): ACCESS / FLOW CONTROL FUNCTIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system isolates security functions enforcing access and information flow control from non-security functions and from other security functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Security function isolation occurs as a result of implementation; the functions can still be scanned and monitored. Security functions that are potentially isolated from access and flow control enforcement functions include, for example, auditing, intrusion detection, and anti-virus functions.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-160	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems provide the capability to enforce access and flow controls separating security functions and non-security functions. Test: Isolation of security functions enforcing access and information flow control.	

SC-03(03): MINIMIZE NONSECURITY FUNCTIONALITY

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization minimizes the number of non-security functions included within the isolation boundary containing security functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
In those instances where it is not feasible to achieve strict isolation of non-security functions from security functions, it is necessary to take actions to minimize the non-security-relevant functions within the security function boundary. Non-security functions contained within the isolation boundary are considered security-relevant because errors or maliciousness in such software, by virtue of being within the boundary, can impact the security functions of organizational information systems. The design objective is that the specific portions of information systems providing information security are of minimal size/complexity. Minimizing the number of non-security functions in the security-relevant components of information systems allows designers and implementers to focus only on those functions which are necessary to provide the desired security capability (typically access enforcement). By minimizing non-security functions within the isolation boundaries, the amount of code that must be trusted to enforce security policies is reduced, thus contributing to understandability.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-160	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-03(04): MODULE COUPLING AND COHESIVENESS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization implements security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The reduction in inter-module interactions helps to constrain security functions and to manage complexity. The concepts of coupling and cohesion are important with respect to modularity in software design. Coupling refers to the dependencies that one module has on other modules. Cohesion refers to the relationship between the different functions within a particular module. Good software engineering practices rely on modular decomposition, layering, and minimization to reduce and manage complexity, thus producing software modules that are highly cohesive and loosely coupled.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-160	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-03(05): LAYERED STRUCTURES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The implementation of layered structures with minimized interactions among security functions and non-looping layers (i.e., lower-layer functions do not depend on higher-layer functions) further enables the isolation of security functions and management of complexity.	
REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-04: INFORMATION IN SHARED RESOURCES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system prevents unauthorized and unintended information transfer via shared system resources.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS, CMS-MARS-E: Std.1 - Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Std.2 - Ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure.	
SUPPLEMENTAL GUIDANCE	
This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection. This control does not address: (i) information remanence which refers to residual representation of data that has been nominally erased or removed; (ii) covert channels (including storage and/or timing channels) where shared resources are manipulated to violate information flow restrictions; or (iii) components within information systems for which there are only single users/roles. PII: Following use of a shared system resource, ensure that shared system resource(s) is purged of personally identifiable information (PII) to prevent unintended users or processes from accessing PII.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; 5 U.S.C. §552a(b) and (e)(10); OMB Circular A-130, 7.g. and 8.b.(3); 45 C.F.R. §164.312(a)(1); IRS1075; CJIS 5.6	AC-3, AC-4, MP-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing information remnants; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Information system for unauthorized and unintended transfer of information via shared system resources.	

SC-05: DENIAL OF SERVICE PROTECTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system protects against or limits the effects of denial of service attacks by employing appropriate security safeguards.	

CMS-ARS:
The information system protects against or limits the effects of the types of denial of service attacks defined in NIST SP 800-61, Computer Security Incident Handling Guide, and the following websites by employing defined security safeguards (defined in the applicable System Security Plan [SSP]):
- SANS Organization: www.sans.org/dosstep;
- SANS Organization's Roadmap to Defeating Distributed Denial of Service (DDoS): www.sans.org/dosstep/roadmap.php; and
- NIST National Vulnerability Database: http://nvd.nist.gov/home.cfm.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The agency head or his/her designated representative and information security officer shall establish a security strategy that includes perimeter protection.
Std.2 - The Department of Information Resources (DIR) will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize state information resources as specified in Chapters 2054 and 2059, Government Code.

CMS-MARS-E
Std.3 - The organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list.

CMS-ARS:
Cloud
Std.3 - For CSPs, the organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by the JAB.
Std.4 - For CSPs, the organization defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by the JAB).

SUPPLEMENTAL GUIDANCE

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal organizational networks from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may also reduce the susceptibility to denial of service attacks.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; IRS1075; CJIS 5.6	SC-6, SC-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records.
Test: Information system for protection against or limitation of the effects of denial of service attacks.

SC-05(01): RESTRICT INTERNAL USERS

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system restricts the ability of individuals to launch denial of service attacks against other information systems.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE	
Restricting the ability of individuals to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Individuals of concern can include, for example, hostile insiders or external adversaries that have successfully breached the information system and are using the system as a platform to launch cyber-attacks on third parties. Organizations can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). Organizations can also limit the ability of individuals to use excessive information system resources. Protection against individuals having the ability to launch denial of service attacks may be implemented on specific information systems or on boundary devices prohibiting egress to potential target systems.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; security plan; list of denial of service attacks launched by individuals against information systems; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. Test: Automated mechanisms restricting the ability to launch denial of service attacks against other information systems.	

SC-05(02): EXCESS CAPACITY / BANDWIDTH / REDUNDANCY

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer. Test: Automated mechanisms implementing management of information system bandwidth, capacity, and redundancy to limit the effects of information flooding denial of service attacks.	

SC-05(03): DETECTION / MONITORING

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	

The organization: (a) Employs monitoring tools to detect indicators of denial of service attacks against the information system; and (b) Monitors information system resources to determine if sufficient resources exist to prevent effective denial of service attacks.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Organizations consider utilization and capacity of information system resources when managing risk from denial of service due to malicious attacks. Denial of service attacks can originate from external or internal sources. Information system resources sensitive to denial of service include, for example, physical disk storage, memory, and CPU cycles. Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example, instituting disk quotas, configuring information systems to automatically alert administrators when specific storage capacity thresholds are reached, using file compression technologies to maximize available storage space, and imposing separate partitions for system and user data.

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	CA-7, SI-4

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with detection and monitoring responsibilities. Test: Automated mechanisms/tools implementing information system monitoring for denial of service attacks.

SC-06: RESOURCE AVAILABILITY

Priority: P0	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system protects the availability of resources by allocating resources by priority and/or quota. **CMS-ARS:** The information system protects the availability of resources by allocating (FedRAMP-defined) resources by priority and/or quota (FedRAMP-defined), and other FedRAMP-defined safeguards for this control.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the CSP control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Test: Automated mechanisms implementing resource allocation capability.

SC-07: BOUNDARY PROTECTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system:
a. Monitors and controls communications at the external boundary, both physically and logically, of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS, CMS-MARS-E:
Std.1 - Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required.
Std.2 - Utilize stateful inspection/application firewall hardware and software.
Std.3 - Utilize firewalls from two (2) or more different vendors at the various levels within the network to reduce the possibility of compromising the entire network.

CMS-ARS:
Std.4 - If the system has an outward facing Web or email presence to the public internet, the organization must implement and support a technical capability to detect malware in web Technical Reference Architecture traffic Technical Reference Architecture traversing the organization's boundary by:
(a) Monitoring assets without the need to deploy software agents(zero client footprint);
(b) Dynamically generating actionable malware intelligence;
(c) Detecting and stopping web-based and e-mail attacks; and
(d) Sending alert data to the organization's SIEM.
Std.5 - Aggregated boundary protection device information must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and, if applicable, federal requirements;
(b) Information sources include boundary protection systems, appliances, devices, services, and applications; and
(c) HHS Information Security directed aggregated boundary protection device information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.6 - As required by HHS, raw boundary protection device information must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZ). Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FIPS Pub: 199; FISCAM: AC-1, AS-2; NIST SP: 800-41, 800-77, 800-137; 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(i); IRS1075; CJIS 5.6	AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; enterprise security architecture documentation; and other relevant documents or records. Examine: Information systems documentation describing boundary protection mechanisms at external connections, between zones, and at the host level. Interview: Selected organizational personnel with boundary protection responsibilities. Test: Mechanisms implementing boundary protection capability within the information system.

SC-07(03): ACCESS POINTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization limits the number of external network connections to the information system.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - Implementation must route external connections via a Trusted Internet Connection (TIC) portal. Cloud: Std.1 - Implementation must be compliant with FedRAMP interconnection requirements.	
SUPPLEMENTAL GUIDANCE	
Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The TIC initiative is an example of limiting the number of external network connections.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; communications and network traffic monitoring logs; other relevant documents or records.	

SC-07(04): EXTERNAL TELECOMMUNICATIONS SERVICES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: (a) Implements a secure managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need. **CMS-MARS** (f) Removed traffic flow policy exceptions that are no longer supported by an explicit mission/business need. **CMS-ARS:**	

(e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of major new system, and removes exceptions that are no longer supported by an explicit mission/business need.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	SC-8

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; traffic flow policy; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; records of traffic flow policy exceptions; and other relevant documents or records. Interview: Selected organizational personnel with boundary protection responsibilities.

SC-07(05): DENY BY DEFAULT / ALLOW BY EXCEPTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.	

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Interview: Selected organizational personnel with boundary protection responsibilities.

SC-07(07): PREVENT SPLIT TUNNELING FOR REMOTE DEVICES

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPN for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need to prevent split tunneling.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records.
Test: Automated mechanisms supporting non-remote connections with the information system.

SC-07(08): ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The information system routes all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at managed interfaces.

CONTROL IMPLEMENTATION STANDARDS

CMS-MARS-E:
Std.1 - The organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing.

CMS-ARS:
Std.1 - For cloud service providers, this Standard replaces the requirement defined in SC-07(08). The information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers within the managed interfaces of boundary protection devices.
Std.2 - For cloud service providers, the organization defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB.

SUPPLEMENTAL GUIDANCE

External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual TCP sessions and blocking specific URLs, domain names, and IP addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AC-3, AU-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records. Test: Mechanisms implementing managed interfaces within information system boundary protection devices

SC-07(11): RESTRICT INCOMING COMMUNICATIONS TRAFFIC

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system only allows incoming communications from authorized sources to be routed to authorized destinations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement provides determinations that source and destination address pairs represent authorized/allowed communications. Such determinations can be based on several factors including, for example, the presence of source/destination address pairs in lists of authorized/allowed communications, the absence of address pairs in lists of unauthorized/disallowed pairs, or meeting more general rules for authorized/allowed source/destination pairs.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities. Test: Automated mechanisms implementing boundary protection capabilities with respect to source/destination address pairs.	

SC-07(12): HOST-BASED PROTECTION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization implements defined, host-based boundary protection mechanisms at defined information system components, including servers, workstations, and mobile devices. **CMS-ARS:** The organization implements FedRAMP defined host-based boundary protection mechanisms at FedRAMP defined information system components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Host-based boundary protection mechanisms include, for example, host-based firewalls. Information system components employing host-based boundary protection mechanisms include, for example, servers, workstations, and mobile devices.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; and other relevant documents or records. Test: Automated mechanisms implementing host-based boundary protection capability.

SC-07(13): ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization defines key information security tools, mechanisms, and support components associated with system and security administration; and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	SA-8, SC-2, SC-3

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal information system components; and other relevant documents or records.

SC-07(14): PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization protects against unauthorized physical connections at those organization-defined managed interfaces necessary to prevent unauthorized physical access, tampering, and theft of PHI.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - The RMH provides implementation standards for managed interfaces.	
SUPPLEMENTAL GUIDANCE	
System interfaces can provide access to the data flows involving PHI. HIPAA has heightened security requirements to protect these interfaces. Under HIPAA, this is an addressable control. Information systems operating at different security categories or classification levels may share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch	

panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items.	
REFERENCES	**RELATED CONTROLS**
Federal: 45 C.F.R. §164.312(e)(1); 45 C.F.R. §164.312(e)(2)(i) ; CJIS 5.6	PE-4, PE-19, RA-3, SI-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the privacy control statements and applicable implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; facility communications and wiring diagram; and other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities. Test: Automated mechanisms supporting and/or implementing protection against unauthorized physical connections.	

SC-07(18): FAIL SECURE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system fails securely in the event of an operational failure of a boundary protection device.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	CP-2, SC-24
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; and other relevant documents or records.	

SC-07(19): BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system blocks both inbound and outbound communications traffic between communication clients that are independently configured by end users and external service providers.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Communication clients independently configured by end users and external service providers include, for example, instant messaging clients. Traffic blocking does not apply to communication clients that are configured by organizations to perform authorized functions.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; list of communication clients independently configured by end users and external service providers; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities. Test: Automated mechanisms supporting and/or implementing the blocking of inbound and outbound communications traffic between communication clients independently configured by end users and external service providers.	

SC-07(21): ISOLATION OF INFORMATION SYSTEM COMPONENTS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs boundary protection mechanisms to separate defined information system components (defined in the applicable System Security Plan) supporting CMS missions and/or business functions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls; separating system components into physically separate networks or subnetworks; cross-domain devices separating subnetworks; virtualization techniques; and encrypting information flows among system components using distinct encryption keys.	
REFERENCES	**RELATED CONTROLS**
	CA-9, SC-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system architecture; information system configuration settings and associated documentation; and other relevant documents or records.	

SC-08: TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): SPI, Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

The information system protects the confidentiality and integrity of transmitted information.

IRS:
The agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel. Network monitoring capabilities must be implemented to detect and monitor for suspicious network traffic. For physical security protections of transmission medium, see Section 9.3.11.4, Access Control for Transmission Medium (PE-4).

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines).

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Any transmitted data containing confidential information must be encrypted using a FIPS 140-2 compliant module (See SC-13).

Web & Mobile:
Std.2 - Where possible, HTTPS should be used for the entire application. If HTTPS use must be limited, then HTTPS must be applied to any authentication pages as well as to all pages after the user is authenticated.
Std.3 - If sensitive information (e.g., personal information) or HHS confidential information can be submitted before authentication, those features must also be sent over HTTPS.
Std.4 - Must use TLS 1.2 or stronger protocols. All other ciphers must be disabled on all servers (e.g., SSLv2, SSLv4, and TLS protocols prior to 1.2.)
Std.5 - Disable the NULL, RC4, DES, and MD5 cipher suites.
Std.6 - Ensure all key lengths are greater than or equal to 128 bits, use secure renegotiation, and disable compression.
Std.7 - Encryption is required whenever the system requests the user enter a user id and password

SPI:
Std.9 - FIPS 140-2 compliant encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.

CMS-ARS, CMS-MARS-E, IRS, CJIS:
Std.1 - Any transmitted data containing confidential information must be encrypted using a FIPS 140-2 validated module (See SC-13).

SUPPLEMENTAL GUIDANCE

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing physical distribution systems) or by logical means (e.g., employing encryption techniques).
Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs) may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk.

PII:
Because of the sensitivity of personally identifiable information (PII) and protected health information (PHI), the confidentiality and integrity of such information in transit must be assured.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy, IS-Web and Mobile Minimum Security Standards, HHS Information Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog	AC-17, PE-4, SI-04, AR-4

Federal: FedRAMP Rev. 4 Baseline; Code: 5 U.S.C. §552a(e)(5) and (10); E-Government Act of 2002 (I; Pub. L. No. 107-347), Title III; FIPS Pub: 140-2, 197; FISCAM: AC-4, AS-2; HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i); 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.312(e)(1); NIST SP: 800-52, 800-77, 800-81, 800-113; OMB Circular A-130: 7.g. and Appendix 1; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems and devices restrict the use of unapproved transmission protocols (including wireless protocols).
Test: Transmission integrity capability within the information system.

SC-08(01): CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

a. The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by Information Security approved alternative safeguards and defined in the applicable System Security Plan (SSP).

IRS:
b. Implement FIPS 140-2 cryptographic mechanisms to prevent unauthorized disclosure of FTI and detect changes to information during transmission across the wide area network (WAN) and within the local area network (LAN)

CMS-MARS-E:
b. This control supports and aligns with the provisions of the ACA and the requirements of 45 CFR §155.260, Privacy and security of personally identifiable information, paragraph (a)(6).

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - Personally identifiable information (PII) must be protected by FIPS-validated encryption or protected distribution systems to ensure the information's confidentiality and integrity during transmission.

SUPPLEMENTAL GUIDANCE

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. However, protected distribution systems can achieve similar results while allowing continuous monitoring of traffic and content through automated DLP systems.

Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

PII:
Because of the sensitivity of PII, the confidentiality and integrity of such information in transit must be assured with encryption techniques if assurance is not provided by other means.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy	SC-13

Federal: Code: 5 U.S.C. §552a(e)(5) and (10); E-Government Act of 2002 (Pub. L. No. 107-347), Title III; FedRAMP Rev. 4 Baseline; OMB Memo: M-07-16 Att. 1, C., M-06-16; OMB Circular A-130: 7.g. and Appendix 1; 45 C.F.R. §164.312(c)(2); 45 C.F.R.§164.312(e)(2)(i); IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Cryptographic mechanisms implementing transmission integrity capability within the information system.

SC-08(02): PRE / POST TRANSMISSION HANDLING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-AS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The information system maintains the confidentiality and integrity of information during preparation for transmission and during reception.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information.

REFERENCES	RELATED CONTROLS
Federal: 5 U.S.C. §552a(e)(5) and (10); OMB Memo: M-07-16, Att. 1, C., M-06-16; OMB Circular A-130: 7.g. and 8.b.(3) and Appendix 1; CJIS 5.6	AC-13, AU-10

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.
Test: Transmission integrity capability within the information system.

SC-10: NETWORK DISCONNECT

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

a. The information system terminates the network connection associated with a communications session at the end of the session or after thirty (30) minutes of inactivity.

CMS-ARS, CMS-MARS-E:
The information system:
a. terminates the network connection associated with a communications session at the end of the session, or:
1. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and
2. Forcibly disconnects inactive VPN connections after thirty (30) minutes or less of inactivity; and

CMS-ARS:
b. terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the HHS CIO, CISO, or Senior Official for Privacy (SOP).

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 - For cloud service providers, this Standard replaces the requirement defined within SC-10. The information system terminates the network connection associated with a communications session at the end of the session, or after thirty (30) minutes for all RAS-based sessions and thirty (30) to sixty (60) minutes for non-interactive users, of inactivity.
Std.2 - For cloud service providers, long running batch jobs and other operations are not subject to this time limit.

IRS:
Std.1 - This control addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect) in contrast to user-initiated logical sessions in AC-12.

SUPPLEMENTAL GUIDANCE

This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of inactivity may be established by organizations and include, for example, time periods by type of network access or for specific network accesses.

A session is an encounter between an end-user interface device (e.g., computer, terminal, process) and an application, including a network logon—the AC-11 session lock applies. A connection-based session is one that requires a connection to be established between hosts prior to an exchange of data.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-40, 800-47, 800-182; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information system functionality include an idle process disconnection capability.
Examine: Information system functionality includes the ability to terminate or suspend communications on a system interconnection.
Test: Network disconnect capability within the information system.

SC-11: TRUSTED PATH

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system establishes a trusted communications path between the user and the security functions of the system

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of organizational information systems. User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. Organizations employ trusted paths for high-assurance connections between security functions of information systems and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-16, AC-25
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing trusted communications paths; security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developer. Test: Automated mechanisms supporting and/or implementing trusted communications paths.	

SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with defined requirements (defined in, or referenced by, the applicable security plan) for key generation, distribution, storage, access, and destruction. **CMS-ARS, CMS-MARS-E:** When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with the HHS Standard for Encryption of Computing Device and organizationally defined requirements (defined in, or referenced by, the applicable System Security Plan) for key generation, distribution, storage, access, and destruction. PII: Because cryptography is desired to protect sensitive information such as personally identifiable information (PII) and protected health information (PHI), cryptographic key establishment and management must be performed in such a way that even the loss of keys will not permit access to the sensitive information. **IRS:** The agency must establish and manage cryptographic keys for required cryptography employed within the information system. Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. **Web & Mobile:** Std.2 - HTTPS certificates should be signed by a reputable certificate authority (e.g. Entrust, Verisign, or an Active Directory CA server). Avoid using self-signed certificates. Std.3 - The name on the certificate should match the fully qualified domain name (FQDN) of the website.	
SUPPLEMENTAL GUIDANCE	

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. **HIPAA:** Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy, IS-Web and Mobile Minimum Security Standards **State:** DIR Security Control Standards Catalog **Federal:** IRS1075; CJIS 5.6	SC-13, SC-17

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Interview: Organizational personnel with responsibilities for cryptographic key establishment or management. Test: Automated mechanisms implementing cryptographic key management and establishment within the information system.

SC-12(01): AVAILABILITY

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization maintains availability of information in the event of the loss of cryptographic keys by users.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Mechanisms are employed to: (a) Prohibit the use of encryption keys that are not recoverable by authorized personnel; (b) Require senior management approval to authorize recovery of keys by other than the key owner; and (c) Comply with approved cryptography standards (see SC-13).	
SUPPLEMENTAL GUIDANCE	
Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).	

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

SC-12(02): SYMMETRIC KEYS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization produces, controls, and distributes symmetric cryptographic keys using NIST-approved key management technology and processes.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
SP 800-57 Part 1-Rev. 4, Recommendation for Key Management, Part 1: General, http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf SP 800-57 Part 3-Rev.1, Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance, http://dx.doi.org/10.6028/NIST.SP.800-	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.	

SC-12(03): ASYMMETRIC KEYS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization produces, controls, and distributes asymmetric cryptographic keys using NIST-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens protecting the user's private key.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
SP 800-57 Part 1-Rev. 4, Recommendation for Key Management, Part 1: General, http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf SP 800-57 Part 3-Rev.1, Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance, http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing cryptographic key management, establishment, and recovery; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Interview: Organizational personnel with responsibilities for cryptographic key establishment or management.	

SC-13: CRYPTOGRAPHIC PROTECTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

When cryptographic mechanisms are used, the information system implements encryption products that are compliant with FIPS 140-2 Cryptographic Module Validation Program (see http://csrc.nist.gov/cryptval/), in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards

CMS-ARS, CMS-MARS-E, IRS, CJIS:
When cryptographic mechanisms are used, the information system implements encryption products that have been validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/cryptval/) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards

CONTROL IMPLEMENTATION STANDARDS

Std.1 **-** The minimum algorithm strength is a 128-bit symmetric encryption algorithm or a comparable strength hashing or asymmetric encryption as determined by the NSA Suite-B Cryptography. This is subject to state organization risk management decisions justified and documented in accordance with TAC 202.21/71(c) and TAC 202.25/75.
Std.2 - Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management, shall be based on documented state organization risk management decisions.
Std.3 - Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted. Confidential information stored in a public location that is directly accessible without compensating controls in place (e.g., FTP without access control) must be encrypted.
Std.4 - Storing confidential information on portable devices is discouraged. Confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-state organization owned computing device.

SUPPLEMENTAL GUIDANCE

Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

This control applies to applications with an integrated access control mechanism, such as WinZip and SecureZip, as well as the underlying operating system. These applications must meet FIPS 140-2 compliant module requirements.

FIPS-validated cryptographic modules are the government standard for encryption. When sensitive information such as PII requires encryption the organization must comply with these standards.

HIPAA:
Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy; HHS Information Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog	AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7

Federal: FIPS Publication 140; Web: http://csrc.nist.gov/cryptval, http://www.cnss.gov; IRS1075; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing use of cryptography; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; and other relevant documents or records.	

SC-15: COLLABORATIVE COMPUTING DEVICES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the HHS CIO or his/her designated representative. If collaborative computer is authorized, the authorization must specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - For cloud service providers, the information system prohibits remote activation of collaborative computing devices with no exceptions. Std.2 - For cloud service providers, the information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.	
SUPPLEMENTAL GUIDANCE	
Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-3, AS-2; IRS1075; CJIS 5.6	AC-21
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users.	

SC-15(01): PHYSICAL DISCONNECT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	

If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Failing to physically disconnect from collaborative computing devices can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure that participants actually carry out the disconnection activity without having to go through complex and tedious procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-47; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems implements functionality that provides an override of interconnections in manner that supports ease of use. Test: Physical disconnect of collaborative computing devices.	

SC-16: TRANSMISSION OF SECURITY ATTRIBUTES

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system associates FBI authorized originating agency identifier (ORI) with information exchanged between information systems and between system components.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address. Std.2 - Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction. Std.3 - Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction	
SUPPLEMENTAL GUIDANCE	
Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-3, AC-4, AC-16
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing transmission of security attributes; access control policy and procedures; information system design documentation; information system	

configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing transmission of security attributes between information systems.

SC-16(01): INTEGRITY VALIDATION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system associates FBI authorized originating agency identifier (ORI) with information exchanged between information systems and between system components.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-3, AC-4, AC-16
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing transmission of security attributes; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing validation of the integrity of transmitted security attributes.	

SC-17: PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization issues public key certificates under a HHS defined certificate policy or obtains public key certificates from an approved service provider. **IRS:** The agency must issue public key infrastructure certificates or obtain public key infrastructure certificates from an approved service provider.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - For cloud service providers, the organization defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.	
SUPPLEMENTAL GUIDANCE	
For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog	SC-12

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-32, 800-63; OMB Memo: M-05-24; IRS1075; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records.
Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities.

SC-18: MOBILE CODE

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the systems if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., smart phones). Mobile code policy and procedures address preventing the development, acquisition, or introduction of unacceptable mobile code within organizational information systems.

REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-4, AS-2; NIST SP: 800-28; IRS1075; CJIS 5.6	AU-2, AU-12, CM-2, CM-6, SI-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records.
Interview: Organizational personnel with mobile code authorization, monitoring, and control responsibilities.
Test: Mobile code authorization and monitoring capability for the organization.

SC-18(01): IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system identifies organization-defined unacceptable mobile code in mobile devices that have a full-feature operating system (i.e. laptops or tables) and ensures, at a minimum the personal firewall performs the actions outlined in Std.1.
CONTROL IMPLEMENTATION STANDARDS
Std.1. At a minimum, the personal firewall shall perform the following activities a. Manage program access to the Internet b. Block unsolicited requests to connect to the user device. c. Filter incoming traffic by IP address or protocol d. Filter incoming traffic by destination ports. e. Maintain an IP traffic log.
SUPPLEMENTAL GUIDANCE
Corrective actions when unacceptable mobile code is detected include, for example, blocking, quarantine, or alerting administrators. Blocking includes, for example, preventing transmission of word processing files with embedded macros when such macros have been defined to be unacceptable mobile code.

REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; list of unacceptable mobile code; list of corrective actions to be taken when unacceptable mobile code is identified; information system monitoring records; information system audit records; other relevant documents or records. Interview: /network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code. Test: Automated mechanisms supporting and/or implementing mobile code detection, inspection, and corrective capability.

SC-18(02): ACQUISITION / DEVELOPMENT / USE

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization ensures that the acquisition, development, and use of mobile code to be deployed in the information system meets organization-defined mobile code requirements.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing mobile code; mobile code requirements; mobile code usage restrictions, mobile code implementation policy and procedures; acquisition documentation; acquisition contracts for information system, system component, or information system service; system development life cycle documentation; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing mobile code; organizational personnel with acquisition and contracting responsibilities. Test: Organizational processes for the acquisition, development, and use of mobile code.

SC-18(03): PREVENT DOWNLOADING / EXECUTION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system prevents the download and execution of organization-defined unacceptable mobile code.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code. Test: Automated mechanisms preventing download and execution of unacceptable mobile code.	

SC-18(04): PREVENT AUTOMATIC EXECUTION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system prevents the automatic execution of mobile code in organization-defined software applications and enforces organization-defined actions prior to executing the code.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Actions enforced before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments. Preventing automatic execution of mobile code includes, for example, disabling auto execute features on information system components employing portable storage devices such as Compact Disks (CDs), Digital Video Disks (DVDs), and Universal Serial Bus (USB) devices.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; information system design documentation; information system configuration settings and associated documentation; list of software applications for which automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code. Test: Automated mechanisms preventing automatic execution of unacceptable mobile code; automated mechanisms enforcing actions to be taken prior to the execution of the mobile code.	

SC-19: VOICE OVER INTERNET PROTOCOL

Priority: P1

Baseline(s): Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

CMS-ARS:
The organization prohibits the use of VoIP technologies, unless explicitly authorized, in writing, by the HHS CIO or his/her designated representative. If VoIP is authorized, the organization:

c. Ensures VoIP equipment used to transmit or discuss sensitive information is protected with HHS (FIPS 140-2 validated module) encryption requirements.

CONTROL IMPLEMENTATION STANDARDS

IRS:
To use a VoIP network that provides FTI to a customer, the agency must meet the following mandatory requirements:
Std.1 - VoIP traffic that contains FTI should be segmented off from non-VoIP
Std.2 - When FTI is in transit across the network (either Internet or state agency's network), the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode
Std.3 - VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in Section 4.0, Secure Storage—IRC 6103(p)(4)(B)
Std.4 - Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements in this publication and is subject to frequent vulnerability testing
Std.5 - VoIP-ready firewalls must be used to filter VoIP traffic on the network
Std.6 - Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter
Std.7 - VoIP phones must be logically protected, and agencies must be able to track and audit all FTI-applicable conversations and access

Additional VoIP guidance is available on the Office of Safeguards website.

SUPPLEMENTAL GUIDANCE

CMS-ARS:
VoIP applications and devices must be configured meet HHS (FIPS 140-2 validated module) requirements. FIPS 140-2 approved security function families are found at http://csrc.nist.gov/groups/STM/cavp/validation.html. However, implementing an approved security function is the start. The product must also be on the approved validation lists. (See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm for a list of current validated products.)

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; NIST SP: 800-58; IRS1075; CJIS 5.6	CM-6, SC-7, SC-15

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records.
Interview: Organizational personnel with VoIP authorization and monitoring responsibilities.
Test: VoIP authorization and monitoring capability for the organization.

SC-20: SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E: Std.1 - Recursive lookups are disabled on all publicly accessible domain name system (DNS) servers.	
SUPPLEMENTAL GUIDANCE	
This control enables external clients including, for example, remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Information systems that provide name and address resolution services include, for example, DNS servers. Additional artifacts include, for example, DNS Security (DNSSEC) digital signatures and cryptographic keys. DNS resource records are examples of authoritative data. The means to indicate the security status of child zones includes, for example, the use of delegation signer resource records in the DNS. The DNS security controls reflect (and are referenced from) OMB Memorandum 08-23. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81; OMB Memo: M-08-23; CJIS 5.6	AU-10, SC-8, SC-12, SC-13, SC-21, SC-22
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information system implements secure resolution services. Examples: 1. DNSSEC 2. Name resolution is configured to maximize security (e.g., disallow recursive lookups as appropriate) Test: Automated mechanisms implementing secure name/address resolution service (authoritative source).	

SC-21: SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.	
SUPPLEMENTAL GUIDANCE	

Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers. Information systems that provide name and address resolution services for local clients include, for example, recursive resolving or caching DNS servers. DNS client resolvers either perform validation of DNS Security (DNSSEC) signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81; CJIS 5.6	SC-20, SC-22
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing data origin authentication and integrity verification for resolution services.	

SC-22: ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information systems that provide name and address resolution services include, for example, domain name system (DNS) servers. To eliminate single points of failure and to enhance redundancy, organizations employ at least two authoritative domain name system servers, one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Organizations specify clients that can access authoritative DNS servers in particular roles (e.g., by address ranges, explicit lists).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-81; CJIS 5.6	SC-2, SC-20, SC-21, SC-24
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; information system design	

documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation.

SC-23: SESSION AUTHENTICITY

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system protects the authenticity of communications sessions.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AC-2, AS-2; NIST SP: 800-52, 800-77, 800-95; IRS1075; CJIS 5.6	SC-8, SC-10, SC-11
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing session authenticity.	

SC-23(01): INVALIDATE SESSION IDENTIFIERS AT LOGOUT

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system invalidates session identifiers upon user logout or other session termination.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the information system invalidates session identifiers upon user logout or other session termination.	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.	

Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing session identifier invalidation upon session termination.

SC-23(03): UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The information system generates a unique session identifier for each session with organization-defined randomness requirements and recognizes only session identifiers that are system-generated.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement curtails the ability of adversaries from reusing previously valid session IDs. Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing session authenticity; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities. Test: Automated mechanisms supporting and/or implementing generating and monitoring unique session identifiers; automated mechanisms supporting and/or implementing randomness requirements.	

SC-24: FAIL IN KNOWN STATE

Priority: P1	
Baseline(s): High	Overlay(s): DIR, CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The information system fails to a known secure state for all failures preserving the maximum amount of state information in failure.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Failure in a known state addresses security concerns in accordance with the mission/business needs of organizations. Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components. Failure in a known safe state helps to prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CP-2, CP-10, CP-12, SC-7, SC-22
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing information system failure; information system design documentation; information system configuration settings and associated documentation; list of failures requiring information system to fail in a known state; state information to be preserved in system failure; other relevant documents or records.	

Test: Automated mechanisms implementing fail-in-known-state capability.

SC-28: PROTECTION OF INFORMATION AT REST

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): SPI, Web & Mobile, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The information system protects the confidentiality and integrity of information at rest in accordance with SC-13 and SC-28(1).

CMS-ARS:
For cloud service providers, the information system enforces encryption of the instance (container) image files under the hypervisor:
- Instance (container) image files from virtual server and client deployments must be encrypted in a manner that meets FIPS 140-2 validated requirements.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Any confidential data stored in the cloud shall be encrypted at rest.

SPI:
Std.2 - The applicant/bidder uses encryption products to protect HHS Confidential Information stored on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.).
Std.3 - FIPS 140-2 compliant encryption is required for Health Insurance Portability and Accountability Act (HIPAA) data, Criminal Justice Information Services (CJIS) data, Internal Revenue Service Federal Tax Information (IRS FTI) data, and Centers for Medicare & Medicaid Services (CMS) data.

Web & Mobile:
Std.4 - Connection strings containing database credentials which are stored in configuration files should be encrypted (e.g. use aspnet_regiis tool to encrypt IIS web.config files).

IRS:
Std.5 - FTI stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.
Std.6 - Mobile devices do require encryption at rest (see Section 9.3.1.14, Access Control for Mobile Devices (AC-19), and Section 9.4.8, Mobile Devices).
Std.7 -The confidentiality and integrity of information at rest shall be protected when located on a secondary (non-mobile) storage device (e.g., disk drive, tape drive) with cryptography mechanisms
Std.8 - Agencies may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms, file share scanning, and integrity protection. Agencies may also employ other security controls, including, for example, secure offline storage in lieu of online storage, when adequate protection of information at rest cannot otherwise be achieved or when continuously monitoring to identify malicious code at rest.

CMS-ARS:
Std.5 - Cloud service providers support the capability to use cryptographic mechanisms to protect information at rest.

CMS-MARS-E:
Std.5 - Sensitive information such as PII should be encrypted while at rest.

SUPPLEMENTAL GUIDANCE

This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of

online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest.

CMS-ARS:
PII:
Because of the sensitivity of PII and protected health information (PHI), the confidentiality and integrity of such information must be assured for data at rest.

HIPAA:
Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the "Safe Harbor" provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; NIST SP: 800-56, 800-57, 800-111; 5 U.S.C. §552a(b) and (e)(10); OMB Memo: M-06-16, M-07-16 Att. 1, C.; 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R.§164.312(e)(2)(ii); IRS1075; CJIS 5.6	AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; and other relevant documents or records.
Test: Automated mechanisms implementing confidentiality and integrity protections for information at-rest.

SC-28(01): CRYPTOGRAPHIC PROTECTION

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, CMS-ARS, CJIS

CONTROL REQUIREMENTS

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of HHS Confidential and Agency Sensitive Information.

CMS-ARS:
PII:
Organizations must:
1. Encrypt data at rest in mobile devices for confidentiality to protect against loss, theft, or compromise;
2. Encrypt data stored in network share drives to insure confidentiality;
3. Encrypt storage/back-up data where physical protection is either not available, not implemented, or not audited;
4. If assurance is not provided by other means, encrypt personally identifiable information (PII) in a database; and
5. Encrypt data stored in the cloud—whether or not the cloud is government or private.

CONTROL IMPLEMENTATION STANDARDS

Web & Mobile:
Std.1 - Connection strings containing database credentials which are stored in configuration files should be encrypted (e.g. use aspnet_regiis tool to encrypt IIS web.config files).

CMS-ARS:

Std.2 - Cloud service providers support the capability to use cryptographic mechanisms to protect information at rest.
SUPPLEMENTAL GUIDANCE
Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. **CMS-ARS:** For additional Guidance, see: US HHS Standard for Encryption of Computing Devices and Information. PII: Because of the sensitivity of PII and PHI, the confidentiality and integrity of such information must be assured for data at rest through the use of encryption technologies if assurance is not provided by other means. Organizations may use file share scanning (e.g., data loss prevention [DLP] technology) to ensure compliance with the requirement to encrypt PII/protected health information (PHI) at rest. **HIPAA:** Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized.

REFERENCES	RELATED CONTROLS
Federal: Code: 5 U.S.C. §552a(b) and (e)(10); FedRAMP Rev. 4 Baseline; OMB Memo: M-06-16, M-07-16 Att. 1, C., 45 C.F.R. §164.312(a)(2)(iv); 45 C.F.R.§164.312(e)(2)(ii); CJIS 5.6	AC-13, AC-19, SC-12

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; procedures addressing protection of information at rest; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; and other relevant documents or records. Test: Automated mechanisms implementing confidentiality and integrity protections for information at-rest.

SC-31: COVERT CHANNEL ANALYSIS

Priority: P1	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert storage and/or timing channels; and b. Estimates the maximum bandwidth of those channels.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems.	

REFERENCES	RELATED CONTROLS
Federal: HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.310(c), 164.312(a), 164.312(e)	AC-3, AC-4, PL-2

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; procedures addressing covert channel analysis; information system design documentation; information system configuration settings and associated documentation; covert channel analysis documentation; information system audit records; other relevant documents or records.
Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with covert channel analysis responsibilities; information system developers/integrators.
Test: Organizational process for conducting covert channel analysis; automated mechanisms supporting and/or implementing covert channel analysis; automated mechanisms supporting and/or implementing the capability to estimate the bandwidth of covert channels.

SC-32: INFORMATION SYSTEM PARTITIONING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization partitions the information system into defined information system components (defined in the applicable System Security Plan [SSP]) residing in separate physical domains or environments based on defined circumstances (defined in the applicable SSP) for physical separation of components.

CONTROL IMPLEMENTATION STANDARDS

CMS-MARS-E:
Std.1 - When contracting with external service providers, Personally Identifiable Information (PII), as well as software and services that receive, process, store, or transmit PII must be isolated within the service provider environment to the maximum extent possible so that other service provider customers sharing physical or virtual space cannot gain access to such data or applications.

CJIS:
Std.1 - The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.
Std.2 -The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:
a. Different computers.
b. Different central processing units.
c. Different instances of the operating system.
d. Different network addresses.
e. Other methods approved by the FBI CJIS ISO.

SUPPLEMENTAL GUIDANCE

Information system partitioning is a part of a defense-in-depth protection strategy. Organizations determine the degree of physical separation of system components from physically distinct components in separate racks in the same room, to components in separate rooms for the more critical components, to more significant geographical separation of the most critical components. Security categorization can guide the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

REFERENCES	RELATED CONTROLS
Federal: FIPS Pub: 199 NIST SP: 800-160; CJIS 5.6	AC-4, SA-8, SC-2, SC-3, SC-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical domains (or environments); information system facility diagrams; other relevant documents or records. Interview: Organizational personnel installing, configuring, and/or maintaining the information system.

SC-36: DISTRIBUTED PROCESSING AND STORAGE

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization distributes, for cloud computing of CJIS information, processing and storage across multiple physical locations.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Distributing processing and storage across multiple physical locations provides some degree of redundancy or overlap for organizations, and therefore increases the work factor of adversaries to adversely impact organizational operations, assets, and individuals. This control does not assume a single primary processing or storage location, and thus allows for parallel processing and storage.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CP-6, CP-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and communications protection policy; contingency planning policy and procedures; contingency plan; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical locations (or environments) with distributed processing and storage; information system facility diagrams; processing site agreements; storage site agreements; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with contingency planning and plan implementation responsibilities; information system developers/integrators. Test: Organizational processes for distributing processing and storage across multiple physical locations; automated mechanisms supporting and/or implementing capability for distributing processing and storage across multiple physical locations.

SC-37: OUT-OF-BAND CHANNELS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization employs FBI defined out-of-band channels for the physical delivery or electronic transmission of information, information system components, or devices to individuals or information systems that process CJIS.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Out-of-band channels include, for example, local (non-network) accesses to information systems, network paths physically separate from network paths used for operational traffic, or non-electronic paths such as the U.S. Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for	

hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; information system design documentation; information system architecture; information system configuration settings and associated documentation; list of out-of-band channels; types of information, information system components, or devices requiring use of out-of-band channels for physical delivery or electronic transmission to authorized individuals or information systems; physical delivery records; electronic transmission records; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; information system developers/integrators. Test: Organizational processes for use of out-of-band channels; automated mechanisms supporting and/or implementing use of out-of-band channels.	

SC-37(01): ENSURE DELIVERY / TRANSMISSION

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization employs FBI defined security safeguards to ensure that only authorized individuals or information systems receive the CJIS information, information system components, or devices.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; information system design documentation; information system architecture; information system configuration settings and associated documentation; list of security safeguards to be employed to ensure designated individuals or information systems receive organization-defined information, information system components, or devices; list of security safeguards for delivering designated information, information system components, or devices to designated individuals or information systems; list of information, information system components, or devices to be delivered to designated individuals or information systems; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; information system developers/integrators.	

Test: Organizational processes for use of out-of-band channels; automated mechanisms supporting and/or implementing use of out-of-band channels; automated mechanisms supporting/implementing safeguards to ensure delivery of designated information, system components, or devices.

SC-38: OPERATIONS SECURITY

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization employs FBI defined operations security safeguards to protect key organizational information throughout the system development life cycle.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Operations security (OPSEC) is a systematic process by which potential adversaries can be denied information about the capabilities and intentions of organizations by identifying, controlling, and protecting generally unclassified information that specifically relates to the planning and execution of sensitive organizational activities. The OPSEC process involves five steps: (i) identification of critical information (e.g., the security categorization process); (ii) analysis of threats; (iii) analysis of vulnerabilities; (iv) assessment of risks; and (v) the application of appropriate countermeasures. OPSEC safeguards are applied to both organizational information systems and the environments in which those systems operate. OPSEC safeguards help to protect the confidentiality of key information including, for example, limiting the sharing of information with suppliers and potential suppliers of information system components, information technology products and services, and with other non-organizational elements and individuals. Information critical to mission/business success includes, for example, user identities, element uses, suppliers, supply chain processes, functional and security requirements, system design specifications, testing protocols, and security control implementation details.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	RA-2, RA-5, SA-12
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing operations security; security plan; list of operations security safeguards; security control assessments; risk assessments; threat and vulnerability assessments; plans of action and milestones; system development life cycle documentation; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; information system developers/integrators. Test: Organizational processes for protecting organizational information throughout the SDLC; automated mechanisms supporting and/or implementing safeguards to protect organizational information throughout the SDLC.	

SC-39: PROCESS ISOLATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system maintains a separate execution domain for each executing process.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – The organization uses operating systems that support process isolation.	
SUPPLEMENTAL GUIDANCE	
Information systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each information system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. This capability is available in most commercial operating systems that employ multi-state processor technologies.	

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline	AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; information system design documentation; information system configuration settings and associated documentation; information system architecture; list of information system physical domains (or environments); information system facility diagrams; other relevant documents or records.
Interview: Organizational personnel installing, configuring, and/or maintaining the information system.

SC-40: WIRELESS LINK PROTECTION

Priority:	
Baseline(s):	Overlay(s): CJIS

CONTROL REQUIREMENTS

The information system protects external and internal wireless links that process CJI from the requirements outlined in Std.1.

CONTROL IMPLEMENTATION STANDARDS

Std.1 – When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:
a. Enable encryption on the hotspot
b. Change the hotspot's default SSID
c. Ensure the hotspot SSID does not identify the device make/model or agency ownership
d. Create a wireless network password (Pre-shared key)
e. Enable the hotspot's port filtering/blocking features if present
f. Only allow connections from agency controlled devices

SUPPLEMENTAL GUIDANCE

This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control.

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	AC-18, SC-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and communications protection policy; access control policy and procedures; procedures addressing wireless link protection; information system design documentation; wireless network diagrams; information system configuration settings and associated documentation; information system architecture; list or internal and external wireless links; list of signal parameter attacks or references to sources for attacks; information system audit records; other relevant documents or records.
Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel authorizing, installing, configuring and/or maintaining internal and external wireless links.
Test: Automated mechanisms supporting and/or implementing protection of wireless links.

SC-43: USAGE RESTRICTIONS

Priority:	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization: a. Establishes usage restrictions and implementation guidance for CJI information stored or process in a cloud environment based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of such components within the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices).	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CM-6, SC-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing usage restrictions; usage restrictions; implementation policy and procedures; authorization records; information system monitoring records; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system. Test: Organizational processes for authorizing, monitoring, and controlling use of components with usage restrictions; Automated mechanisms supporting and/or implementing authorizing, monitoring, and controlling use of components with usage restrictions.	

SC-44: DETONATION CHAMBERS

Priority:	
Baseline(s):	Overlay(s): HIPAA
CONTROL REQUIREMENTS	
The organization employs a detonation chamber capability within organization-defined information system, system component, or location.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).	
REFERENCES	**RELATED CONTROLS**
Federal: HIPAA Security Rule 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	SC-7, SC-25, SC-26, SC-30
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and communications protection policy; procedures addressing detonation chambers; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records.	

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system. Test: Automated mechanisms supporting and/or implementing detonation chamber capability.

SC-CMS-01, SC-ACA-01: ELECTRONIC MAIL

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
Controls must be implemented to protect sensitive information that is sent via email.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-MARS-E Std.1 – Prior to sending an email, place all sensitive information in an encrypted attachment **CMS-ARS:** Std.1 - Email and any attachment that contains sensitive information when transmitted inside and outside of HHS premises shall be encrypted using the user's Personal Identity Verification (PIV) card when possible. If PIV encryption is not feasible, a FIPS 140-2 validated solution must be employed: - Password protection of files are recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions. - Password and/or encryption key shall not be included in the same email that contains sensitive information or in separate email. Password/encryption key shall be provided to the recipient separately via text message, verbally, or other out-of-band solution. Std.2 - MFA is required before being granted access to CMS email. Std.3 - MFA access control mechanisms must meet CMS approved standards discussed in the RMH, Volume III, Standard 3.1, CMS Authentication Standards.	
SUPPLEMENTAL GUIDANCE	
For guidance and recommended security practices for handling sensitive information via e-mail see NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.	
REFERENCES	**RELATED CONTROLS**
Federal: HSPD: HSPD-12; NIST SP: 800-45	SI-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Email policy and procedures; and other relevant documents or records. Examine: Information system enforces approved multifactor authentication for access to email. Interview: Sample of organizational personnel who use email.	

SC-CMS-02: WEBSITE USAGE

Priority: P2	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
Websites are operated within the restrictions addressed in OMB directives M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," M-15-13, "Policy to Require Secure Connections across Federal Websites and Web Services," and applicable CMS and HHS directives and instruction.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - All publicly accessible federal websites and web services shall employ secure connections, such as Hypertext Transfer Protocol Secure (HTTPS). Std.2 - TLS shall be implemented and configured in accordance with the recommendation of NIST SP 800-52, as amended. Std.3 - Websites and services shall deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices protocol versions, and other configuration elements. Std.4 - Websites and services available over HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS going forward.	

Std.5 - Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections shall be acceptable and encouraged. HSTS headers must specify a max-age of at least 1 year.	
SUPPLEMENTAL GUIDANCE	
Monitor the CMS and HHS security programs to determine if there are any modified directives and instruction.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-10-22, M-10-23, M-15-13	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: CMS web site baseline and change management documentation for appropriate configurations. Interview: Web site administrators.	

SC-ACA-02: FAX USAGE

Priority:	
Baseline(s):	Overlay(s): CMS-MARS-E
CONTROL REQUIREMENTS	
If Personally Identifiable Information (PII) is allowed to be included with fax communications, the organization establishes policies and procedures for handling fax transmissions. The organization must follow specific precautions and Implementation Standards when performing fax transmission of PII: a. Transmit PII only to an authorized recipient	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - When sending or receiving faxes containing PII: a. Fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; b. Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and c. A cover sheet must be used that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.	
SUPPLEMENTAL GUIDANCE	
Do not send PII over FAX unless it cannot be sent over other, more secure, channels, i.e., delivery by hand, secure email, etc.	
REFERENCES	**RELATED CONTROLS**
	PE-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of the SC-ACA-2 control as described in the control requirements and associated implementation standards.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Fax handling policy and procedures addressing the protection of PII. Examine: Fax machine locations for secure custodial coverage of outgoing and incoming PII transmitted data. Interview: Organizational personnel with responsibility for security and organizational personnel with responsibility for handling fax transmissions.	

(SI) SYSTEM AND INFORMATION INTEGRITY

The HHS organization provides oversight to ensure (i) the identification, reporting, and the correction of information system flaws in a timely manner; (ii) protection from malicious code at appropriate locations within HHS information systems; and (iii) the monitoring of information system security alerts and advisories, and execution of appropriate actions.

SI-01: SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates (as necessary) the current:
1. System and information integrity policy at least every three (3) years; and
2. System and information integrity procedures at least every three hundred and sixty five (365) days.

CMS-MARS-E:
b.1. 1. System and information integrity policy at least every three hundred and sixty five (365) days

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The integrity of data, its source, its destination, and processes applied to it shall be assured. Changes to data shall be made only in an authorized manner.

SUPPLEMENTAL GUIDANCE

This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

PII:
Policies that support protecting the integrity of systems and information are necessary to meet the Privacy Act requirements to protect against any anticipated threats or hazards to the security or integrity of records.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b)and (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AS-1, SM-1, SM-3; HIPAA: 45 C.F.R. §164.312(c)(1); 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii); NIST SP: 800-12, 800-100; OMB Memo: M-07-16; IRS1075; CJIS 5.6	PM-9

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy and procedures; other relevant documents or records.
Interview: Organizational personnel with system and information integrity responsibilities.

SI-02: FLAW REMEDIATION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): SPI, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Identifies, reports, and corrects information system flaws;

b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates as directed in Implementation Standard 1; and
d. Incorporates flaw remediation into the organizational configuration management process.

CMS-ARS, IRS:
e. Centrally manages the flaw remediation process

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Correct identified security-related information system flaws using timelines established by the CISO. Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes; and
Std.2 - A risk-based decision is documented in the form of a risk exception and documented in the risk analysis and security plan if a security patch is not to be applied to an information technology component or a legacy (no-longer maintained by the vendor) component is to remain in use.
Std.3 - Flaw remediation requirements apply to all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE -identified vulnerability.
Std.4 - The organization must provide timely responses, as defined by the CISO, to informational requests for organizational flaw (e.g., patch) status and posture information.

SPI:
Std.5 - The applicant/bidder keeps current on security updates/patches (including firmware, software, and applications) for computing systems that use, disclose, access, create, transmit, maintain, or store HHS Confidential Information.

CMS-ARS:
Std.1 - Correct identified security-related information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days.

CMS-MARS-E:
Std. 1 - The organization installs security-relevant software and firmware updates on production equipment within a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw as follows: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days.

SUPPLEMENTAL GUIDANCE

Organizations identify information systems affected by announced software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, and hot fixes. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow United States Computer Emergency Readiness Team (US-CERT) guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors, including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates are not necessary or practical. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.
Operating systems and installed applications, including databases and services, need to be examined.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy, Information Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog	CA-2, CA-7, CM-3, CM-5, CM-8, IR-4, MA-2, RA-5, SA-10, SA-11, SI-11

Federal: FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R. §164.308(a)(5)(ii)(B); NIST SP: 800-40, 800-37, 800-39, 800-137, 800-182; OMB Memo: M-14-03, M-15-01, M-16-04; IRS1075 9.3.17.2; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; and other relevant documents or records.
Examine: Information systems are patched within time-frame requirements and patch logs show system is being maintained within required time-frames.
Interview: Organizational personnel with flaw remediation responsibilities.

SI-02(01): CENTRAL MANAGEMENT

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization centrally manages the flaw remediation process.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Automated flaw remediation results must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Flaw remediation results sources include all information technology components for which a patch or work-around exists for each vendor-identified and/or CVE/CWE-identified vulnerability; and
(c) HHS Information Security directed flaw remediation information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 - As required by CMS, raw security information/results from automated flaw remediation tools must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.

REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; and other relevant documents or records.
Examine: Information systems demonstrate automated mechanisms are used to remediate flaws.
Test: Mechanisms supporting centralized management of flaw remediation and automatic software updates.

SI-02(02): AUTOMATED FLAW REMEDIATION STATUS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS	
The organization employs automated mechanisms monthly to determine the state of information systems with regard to flaw remediation. **CMS-ARS:** The organization employs automated mechanisms no less often than once every seventy-two (72) hours to determine the state of information system components with regard to flaw remediation.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	CM-6, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; and other relevant documents or records. Examine: Information systems include capability to evaluate flaw remediation within the stated time period. Test: Automated mechanisms implementing information system flaw remediation update status.	

SI-02(03): TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization: a. Measures the time between flaw identification and flaw remediation; and b. Corrective actions must be taken within the time periods defined under the SI-2 (Flaw Remediation) Implementation Standards.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; and other relevant documents or records. Interview: Organizational personnel with responsibility for flaw remediation; organizational personnel with configuration management responsibility. Test: Automated mechanisms supporting and/or implementing reporting, and correcting information system flaws; automated mechanisms supporting and/or implementing testing software and firmware updates.	

SI-03: MALICIOUS CODE PROTECTION

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlays(s): SPI, DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with HHS configuration management policy and procedures; and
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system using the frequency specified in Implementation Standards, and real-time scans of files from external sources at endpoint, and/or network entry/exit points, as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

CONTROL IMPLEMENTATION STANDARDS

Std.1 **-** Perform periodic scans of the HHS information systems every twenty-four (24) hours, and real-time scans of files from external sources at endpoints as the files are downloaded, opened, or executed in accordance with HHS organizational security policy; and;

SPI:
Std.2 - The applicant/bidder's computing systems that use, disclose, access, create, transmit, maintain, or store HHS Confidential Information contains up-to-date anti-malware and antivirus protection.

CMS-ARS
Std.1 - Desktop malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.3 - Server (to include databases and applications) malicious code scanning software is configured to perform critical system file scans no less often than once every twelve (12) hours and full system scans no less often than once every seventy-two (72) hours.
Std.4 - Malicious code scanning results are reported to HHS Information Security SIEM in compliance with AU-06.
Std.5 - For Cloud Service Providers the organization configures malicious code protection mechanisms to:
- Perform periodic scans of the information system at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- Block or quarantine malicious code, send alert to administrator, send alert to FedRAMP in response to malicious code detection.

SUPPLEMENTAL GUIDANCE

Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means, including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards, including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different

actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. **HIPAA:** Malicious code protections are essential in system with PHI because of the sensitivity and desirability of such information. Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy; Information Security and Privacy Initial Inquiry (SPI) **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; NIST SP: 800-37, 800-39, 800-83, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04; 45 C.F.R. §164.308(a)(5)(ii)(B); 45 C.F.R. §164.308(a)(6)(ii); IRS1075; CJIS 5.6	CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems, databases, and applications employ malicious code protection mechanisms. Examine: Information systems, databases, and applications employ periodic scans for malicious code. Interview: Organizational personnel with malicious code protection responsibilities. Test: Automated mechanisms implementing malicious code protection capability.	

SI-03(01): CENTRAL MANAGEMENT

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization centrally manages malicious code protection mechanisms.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw, malicious code protection security controls.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AU-2, SI-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.	

SI-03(02): AUTOMATIC UPDATES

Priority: P1

Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system automatically updates malicious code protection mechanisms (including signature definitions).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	SI-8
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records.	

SI-03(07): NONSIGNATURE-BASED DETECTION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements non-signature-based malicious code detection mechanisms.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for malicious code protection. Test: Automated mechanisms supporting and/or implementing non-signature-based malicious code protection capability.	

SI-04: INFORMATION SYSTEM MONITORING

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with the current HHS monitoring objectives; and	

2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through defined techniques and methods (defined in the applicable System Security Plan);
c. Deploys monitoring devices:
1. Strategically within the information system to collect organization-determined essential information; and
2. At ad hoc locations within the system to track specific types of transactions of interest to the organization.
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides defined information system monitoring information (defined in the applicable System Security Plan) to defined personnel or roles (defined in the applicable System Security Plan) as needed, and at defined frequency (defined in the applicable System Security Plan).

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Each state organization head or his/her designated representative and information security officer shall establish a security strategy that includes perimeter protection.
Std.2 - The Department of Information Resources (DIR) will provide security information management services to include external network monitoring, scanning, and alerting for state organizations that utilize State information resources as specified in Chapters 2054 and 2059, Government Code. Perimeter security controls may include some or all of the following components: DMZ, firewall, intrusion detection or prevention system, or router.
Std.3 - Install Intrusion Detection"/Prevention" System (IDS"/IPS") devices at network perimeter points and host-based IDS"/IPS" sensors on critical servers.

CMS-ARS:
Std.4 - Implement a centrally managed IDS or IPS capability to monitor network communications on all networks and subnets of any environment requiring a HHS Authority to Operate.
a. Permitted IDS/IPS mechanisms:
- centrally managed IDS/IPS devices at network perimeter points, to include between zones; and
- centrally managed host-based IDS/IPS sensor agents in information technology components for which such agents are available.
b. Environments where communications within the zone are encrypted must use mechanisms capable of either decrypting content for analysis or analyzing content before Technical Reference Architecture transmission/after receipt; and
c. Information technology components that do not support a host-based IDS/IPS sensor capability must be documented in the applicable risk assessment and security plan.
Std.5 - Monitoring functionality supports the sharing of threat awareness information in a format that meets HHS requirements.
Std.6 - The organization monitors for unauthorized remote connections to the information system continuously, in real-time and takes appropriate action if an unauthorized connection is discovered.
Std.7 - For cloud service providers, the organization monitors events on the information system to ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examines system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifies irregularities or anomalies that are indicators of a system malfunction or compromise; and detects information system attacks.

SUPPLEMENTAL GUIDANCE

Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real-time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from DHS can also be included as monitoring devices. The granularity of monitoring information collected is based on

organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, HTTP traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

PII:
Intrusion-monitoring tools may collect personally identifiable information (PII) of all types. Notice to users who are monitored should be provided prior to system use. Controls sufficient to protect the type of PII collected must be in place for the technology performing the monitoring, including encryption of monitoring data that may contain PII. When conducting information system monitoring on internal or external networks which may collect PII, the organization should coordinate with the organization's counsel and privacy officer.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(b), (e)(10); FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2; HIPAA: 45 C.F.R. §164.308(a)(1)(ii)(D), 45 C.F.R. §164.308(a)(5)(ii)(B), 45 C.F.R. §164.308(a)(6)(ii); NIST SP: 800-61, 800-83, 800-92, 800-94, 800-137; OMB Memo: M-07-16, M-14-03, M-15-01, M-16-04; OMB Circular A-130: 7.g.; IRS1075; CJIS 5.6	AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports monitoring to detect attacks and indicators of potential attacks.
Interview: Organizational personnel with information system monitoring responsibilities.
Test: Automated mechanisms supporting and/or implementing information system monitoring capability.

SI-04(01): SYSTEM-WIDE INTRUSION DETECTION SYSTEM

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Low, Low Plus, Moderate, High:
Std.1 – Aggregated intrusion detection information must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and
(b) Information sources include all network and host-based IDS/IPS capabilities monitoring network communications on all networks and subnets of any environment requiring a CMS Authority to Operate.
Std.2 – As required by CMS, raw intrusion detection information must be available in an unaltered format to HHS Information Security.

High:
Std.1 – Aggregated intrusion detection information must be searchable by HHS Information Security:
(c) HHS Information Security directed aggregated intrusion detection information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.

SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing information system intrusion detection tools and techniques; information system design documentation; information system intrusion detection tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports intrusion detection at external connections, between zones, and at the host level.
Interview: Organizational personnel with information system monitoring responsibilities.
Test: Automated mechanisms supporting and/or implementing Information system-wide intrusion detection capability.

SI-04(02): AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization employs automated tools to support near real-time analysis of events.

CONTROL IMPLEMENTATION STANDARDS

CMS-ARS:
Std.1 – Aggregated real-time analysis of events information must be searchable by HHS Information Security:
(a) Information is provided to HHS Information Security in a format compliant with HHS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements;
(b) Information sources include events/notifications emanating from local analysis tools and directly from any information technology component in an environment requiring a HHS Authority to Operate; and
(c) HHS Information Security directed real-time analysis of events information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request.
Std.2 – As required by HHS, raw event information must be available in an unaltered format to HHS Information Security.

SUPPLEMENTAL GUIDANCE

Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or security information and event management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

REFERENCES	RELATED CONTROLS
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01; CJIS 5.6	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).

ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; and other relevant documents or records.
Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports near real-time analysis of events.
Test: Automated tools supporting near real-time event analysis.

SI-04(03): AUTOMATED TOOL INTEGRATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; and other relevant documents or records. Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports integration of intrusion detection tools into access control and flow control mechanisms. Test: Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms	

SI-04(04): INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system monitors inbound and outbound communications traffic at a defined frequency (defined in the applicable System Security Plan) for unusual or unauthorized activities or conditions.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – Aggregated inbound and outbound communications Technical Reference Architecture traffic information must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; (b) Information sources include Technical Reference Architecture traffic analysis information from local analysis tools and directly from any information technology component in an environment requiring a CMS Authority to Operate; and (c) HHS Information Security directed aggregated inbound and outbound communications Technical Reference Architecture traffic information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 – As required by CMS, raw event information must be available in an unaltered format to HHS Information Security.	
SUPPLEMENTAL GUIDANCE	
Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; and other relevant documents or records. Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that supports monitoring of inbound and outbound communications traffic at a defined frequency. Test: Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.

SI-04(05): SYSTEM-GENERATED ALERTS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system alerts defined personnel or roles (defined in the applicable System Security Plan) when the following indications of compromise or potential compromise occur: a. Presence of malicious code; b. Unauthorized export of information; c. Signaling to an external information system; or d. Potential intrusions.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: <u>Low, Low Plus, Moderate, High</u>: Std.1 – Aggregated alert information must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and Federal (e.g., Continuous Diagnostics and Mitigation) requirements; and (b) Information sources include all alert-generating information technology components in an environment requiring a CMS Authority to Operate. Std.2 – As required by CMS, raw event information must be available in an unaltered format to HHS Information Security. <u>Moderate, High</u>: Std.1 – (c) HHS Information Security directed aggregated alert information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. <u>Cloud</u>: Std.3 – For cloud service providers, this Standard replaces the requirement defined within SI-04(05). The indications that a compromise or potential compromise occurred include: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose. Std.4 – For cloud service providers, the organization defines additional compromise indicators as needed.	
SUPPLEMENTAL GUIDANCE	
Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/Information Owner(s)/Custodian(s), system owners, or information system security officers.	

Cloud: Alerts may be generated from a variety of sources, including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-137; OMB Memo: M-14-03, M-15-01; CJIS 5.6	AU-5, PE-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems employ automated functionality (as systems, devices, appliances or applications) that provides alerts to defined personnel or roles (defined in the applicable System Security Plan) when any of the organization-defined list of compromise or potential compromise indicators occur. Test: Information system monitoring real-time alert capability.	

SI-04(07): AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

Priority: P1	
Baseline(s):	Overlay(s): IRS, CJIS
CONTROL REQUIREMENTS	
Notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AU-5, PE-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; alerts/notifications generated based on detected suspicious events; records of actions taken to terminate suspicious events; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing notifications to incident response personnel; automated mechanisms supporting and/or implementing actions to terminate suspicious events.	

SI-04(09): TESTING OF MONITORING TOOLS

Priority: P1	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization tests intrusion-monitoring tools.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations. The frequency of testing depends on the types of tools used by organizations and methods of deployment.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	CP-9
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing testing of information system monitoring tools and techniques; documentation providing evidence of testing intrusion-monitoring tools; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing testing of intrusion-monitoring tools.	

SI-04(11): ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES

Priority: P1	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization analyzes outbound communications traffic at the external boundary of the information system and interior points within the system (e.g., subnetworks, subsystems) that process CJI to discover anomalies.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – Monitor inbound and outbound communications for unusual or unauthorized activities. Std.2 – Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort. Std.3 – Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.	
SUPPLEMENTAL GUIDANCE	
Anomalies within organizational information systems include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; network diagram; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system monitoring logs or records; information system audit records; other relevant documents or records.	

Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing analysis of communications traffic.

SI-04(12): AUTOMATED ALERTS

Priority: P1	
Baseline(s):	Overlay(s): IRS, CJIS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement focuses on the security alerts generated by organizations and transmitted using automated means. In contrast to the alerts generated by information systems in SI-4(5), which tend to focus on information sources internal to the systems (e.g., audit records), the sources of information for this enhancement can include other entities as well (e.g., suspicious activity reports, reports on potential insider threats).	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-18, IA-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; list of inappropriate or unusual activities (with security implications) that trigger alerts; alerts/notifications provided to security personnel; information system monitoring logs or records; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing automated alerts to security personnel.	

SI-04(14): WIRELESS INTRUSION DETECTION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; GAO finding; CJIS 5.6	AC-18, IA-3
ASSESSMENT PROCEDURES	

ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Organization employs wireless intrusion detection functionality (as systems, devices, appliances or applications) that supports identification of rogue wireless devices. Interview: Organizational personnel with information system monitoring responsibilities. Test: Wireless intrusion detection mechanisms.

SI-04(15): WIRELESS TO WIRELINE COMMUNICATIONS

Priority: P1	
Baseline(s):	Overlay(s): CJIS
CONTROL REQUIREMENTS	
The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: CJIS 5.6	AC-18
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; information system audit records; other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring the information system; organizational personnel with responsibility for the intrusion detection system. Test: Organizational processes for intrusion detection/information system monitoring; automated mechanisms supporting and/or implementing intrusion detection/information system monitoring capability; automated mechanisms supporting and/or implementing wireless intrusion detection capability.	

SI-04(16): CORRELATE MONITORING INFORMATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization correlates information from monitoring tools employed throughout the information system.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: Cybersecurity Enhancement Act of 2014; FedRAMP Rev. 4 Baseline; OMB Memo: M-14-03, M-15-01	AU-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	

Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; procedures addressing security monitoring tool data correlation; and other relevant documents or records. Examine: Organization employs automated tools to correlate security monitoring tool data collected throughout the information system. Interview: Organizational personnel with information system monitoring responsibilities.

SI-04(23): HOST-BASED DEVICES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, IRS
CONTROL REQUIREMENTS	
The organization implements host-based monitoring mechanisms on all systems, appliances, devices, services, and applications; **CMS-ARS, CMS-MARS-E:** Devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability must be documented in the applicable Information System Risk Assessment and System Security Plan.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; NIST SP: 800-37, 800-39, 800-137; OMB Memo: M-14-03, M-15-01, M-16-04	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; and other relevant documents or records. Examine: Information systems and/or networks employ host-based monitoring mechanisms. Test: Information system monitoring real-time alert capability.	

SI-04(24): INDICATORS OF COMPROMISE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system discovers, collects, distributes, and uses indicators of compromise.	
CONTROL IMPLEMENTATION STANDARDS	
Moderate: Std.1 - Indicators of compromise IOCs information must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and federal (e.g., OpenIOC, STIX, CybOX, TAXII) requirements; and (b) IOCs sources include internal development, commercial/industry organizations and groups (e.g., ISAC, IOC Bucket) and security-related entities. Std.2 - As required by CMS, IOC information must be available in an unaltered format to HHS Information Security. High:	

Std.1 - indicators of compromise (IOC) information must be searchable by HHS Information Security: (a) Information is provided to HHS Information Security in a format compliant with CMS and federal (e.g., OpenIOC, Structured Threat Information eXpression [STIX], Cyber Observable eXpression [CybOX], Trusted Automated eXchange of Indicator Information [TAXII]) requirements; (b) IOCs sources include internal development, commercial/industry organizations and groups (e.g., Information Sharing and Analysis Center [ISAC], indicators of Compromise [IOC] Bucket) and security-related entities; and (c) HHS Information Security directed IOCs information collection rules/requests (e.g., sources, queries, data calls) must be implemented/provided within the timeframe specified in the request. Std.2 - As required by CMS, IOC information must be available in an unaltered format to HHS Information Security.
SUPPLEMENTAL GUIDANCE
IOCs are forensic artifacts from intrusions that are identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. IOCs for the discovery of compromised hosts can include for example, the creation of registry key values. IOCs for network traffic include, for example, URL or protocol elements that indicate malware command and control servers. The rapid distribution and adoption of IOCs can improve information security by reducing the time that information systems and organizations are vulnerable to the same exploit or attack. See also: http://www.issa.org/resource/resmgr/journalpdfs/feature0515.pdf

REFERENCES	RELATED CONTROLS
Federal: Cybersecurity Enhancement Act of 2014; NIST SP: 800-61, 800-83, 800-92, 800-94, 800-137	IR-10

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the information system: - discovers indicators of compromise; - collects indicators of compromise; - distributes indicators of compromise; and - uses indicators of compromise.
ASSESSMENT METHODS AND OBJECTS
Examine: System and information integrity policy; procedures addressing information system monitoring; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system monitoring logs or records; information system audit records; and other relevant documents or records. Interview: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the information system; organizational personnel with responsibility for monitoring information system hosts. Test: Organizational processes for information system monitoring; organizational processes for discovery, collection, distribution, and use of indicators of compromise; automated mechanisms supporting and/or implementing system monitoring capability; automated mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise.

SI-05: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Priority: P1	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Receives information system security alerts, advisories, and directives from defined external organizations (including US-CERT and organizations as defined in the applicable System Security Plan) on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: defined personnel or roles; and d. Implements security directives in accordance with established time frames or notifies issuing organization of the degree of noncompliance.	
CONTROL IMPLEMENTATION STANDARDS	
CMS-ARS: Std.1 - The organization's security operations center is responsible for responding to advisories, requests, or directives issued by the CMS Security Operations Center (SOC) and/or HHS Information Security.	

Std.2 - For cloud service providers, the organization disseminates security alerts, advisories, and directives to all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP. Std.3 - For cloud service providers, the organization defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.
SUPPLEMENTAL GUIDANCE
The US-CERT generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. PHI: Receiving and acting on security alerts from US-CERT, or other appropriate organizations, assists in protecting PHI by protecting information systems against rapidly evolving threats. Under HIPAA, this is an addressable control.

REFERENCES	RELATED CONTROLS
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** NIST Special Publication 800-40; IRS1075; CJIS 5.6	SI-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS
Examine: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; and other relevant documents or records. Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system.

SI-05(01): AUTOMATED ALERTS AND ADVISORIES

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CJIS
CONTROL REQUIREMENTS	
The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk, including the governance level, mission/business process/enterprise architecture level, and the information system level.	

REFERENCES	RELATED CONTROLS
Federal: CJIS 5.6	

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).
ASSESSMENT METHODS AND OBJECTS

Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records. Test: Automated mechanisms implementing the distribution of security alert and advisory information.

SI-06: SECURITY FUNCTION VERIFICATION

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system: a. Verifies the correct operation of defined security functions (defined in the applicable System Security Plan); b. Performs this verification upon system startup, restart, and upon command by a user with appropriate privileges no less often than once per month; c. Notifies the system administrators of failed security verification tests; and d. Shuts the information system down, or restarts the information system, or performs some other defined alternative action(s) (defined in the applicable System Security Plan) when anomalies are discovered.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For cloud service providers, the information system verifies the correct operation of security functions upon system startup and/or restart and periodically every thirty (30) days and notifies system administrator and performs FedRAMP and CMS-defined actions when anomalies are discovered.	
SUPPLEMENTAL GUIDANCE	
Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; FISCAM: AC-5, AS-2	CA-7, CM-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records. Test: Security function verification capability.	

SI-06(02): AUTOMATION SUPPORT FOR DISTRIBUTED TESTING

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements automated mechanisms to support for the management of distributed security testing.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	SI-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; security plan; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms supporting the management of distributed security function testing.

SI-07: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): HIPAA, CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization employs integrity verification tools to detect unauthorized changes to software, firmware, and information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. PII: Detection of unauthorized changes to sensitive information such as personally identifiable information (PII) and systems containing sensitive information is fundamental to ensuring integrity as required by the Privacy Act	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-4; HIPAA: 45 C.F.R. §164.312(c)(1), 45 C.F.R. §164.312(c)(2), 45 C.F.R. §164.312(e)(2)(i), 45 C.F.R. §164.312(c), 45 C.F.R.; NIST SP: 800-147, 800-155; Code: 5 U.S.C. §552a(e)(5); OMB Memo: M-04-04; OMB Circular A-130: 7.g., and Appendix II; CJIS 5.6	SA-12, SC-8, SC-13, SI-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records.	

SI-07(01): INTEGRITY CHECKS

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The information system performs an integrity check of software, firmware, and information daily and at system startup.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For cloud service providers, the organization reassesses the integrity of software and information by performing no less often than one monthly scans of the information system.	
SUPPLEMENTAL GUIDANCE	
Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.	
REFERENCES	**RELATED CONTROLS**

Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and information integrity; security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.	

SI-07(02): AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization employs automated tools that provide notification to defined personnel or roles (defined in the applicable System Security Plan) upon discovering discrepancies during integrity verification.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/Information Owner(s)/Custodian(s), information system owners, systems administrators, software developers, systems integrators, and information security officers.	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.	

SI-07(05): AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system automatically implements one or more of the security safeguards defined in Implementation Standard 1 when integrity violations are discovered. Implemented safeguards must be specified in the applicable System Security Plan.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - One or more of the following safeguards must be implemented: (a) Shuts the information system down; (b) Restarts the information system; or (c) Implements the security safeguards defined in the System Security Plan.	
SUPPLEMENTAL GUIDANCE	
Organizations may define different integrity checking and anomaly responses: (i) By type of information (e.g., firmware, software, user data); (ii) By specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) A combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.	
REFERENCES	**RELATED CONTROLS**

ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.	

SI-07(06): CRYPTOGRAPHIC PROTECTION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information. FIPS-validated cryptography must be used to detect unauthorized changes to software, firmware, and information.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
PII: Detection of unauthorized changes to sensitive information such as personally identifiable information (PII) and systems containing sensitive information is fundamental to ensuring data integrity. FIPS-validated cryptographic modules are the government standard for integrity verification. When PII requires integrity verification the organization must comply with these standards. Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. **HIPAA:** Under HIPAA, encryption is an addressable control. However, using cryptographic protection allows the organization to utilize the “Safe Harbor” provision under the Breach Notification Rule. If PHI is encrypted pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (45 C.F.R. Part 164 Subpart D), then no breach notification is required following an impermissible use or disclosure of the information. Therefore, organizations should use cryptographic protections for PHI stored on electronic media	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(10); OMB Memo: M-07-16, Att. 1, C, M-04-04; OMB Circular A-130: 7.g. and Appendix II; 45 C.F.R. §164.312(c); 45 C.F.R. §164.312	SC-13
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the PII control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software, firmware, and information integrity; information system design documentation; information system configuration settings and associated documentation; cryptographic mechanisms and associated documentation; records of detected unauthorized changes to software, firmware, and information; information system audit records; and other relevant documents or records. Interview: Organizational personnel with responsibility for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer. Test: Software, firmware, and information integrity verification tools; cryptographic mechanisms implementing software, firmware, and information integrity.	

SI-07(07): INTEGRATION OF DETECTION AND RESPONSE

Priority: P1	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization incorporates the detection of defined unauthorized security-relevant changes (defined in the applicable System Security Plan) to the information system into the organizational incident response capability.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	IR-4, IR-5, SI-4
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records.	

SI-07(14): BINARY OR MACHINE EXECUTABLE CODE

Priority: P1	
Baseline(s): High	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Prohibits the use of binary or machine executable code from sources with limited or no warranty and without the provision of source code; and b. Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
	SA-5
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing software and source code acquisition; information system design documentation; information system software component inventory; documentation of exceptions to the control's source code requirement; other relevant documents or records. Interview: Organizational personnel with development and integration responsibilities.	

SI-08: SPAM PROTECTION

Priority: P2

Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means, including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. **HIPAA:** HIPAA requires organizations to implement procedures for guarding against, detecting and reporting malicious software which can be introduced to the system through spam. Under HIPAA, this is an addressable control.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: AS-3, CM-5; HIPAA: 45 C.F.R.§164.308(a)(5)(ii)(B); 45 C.F.R.§164.308(a)(6)(ii) NIST SP: 800-45; IRS1075; CJIS 5.6	AT-3, SC-5, SC-7, SI-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records. Interview: Organizational personnel with spam protection responsibilities. Test: Automated mechanisms implementing spam detection and handling capability.	

SI-08(01): CENTRAL MANAGEMENT

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization centrally manages spam protection mechanisms.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls.	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	AU-3, SI-2, SI-7
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	

Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.

SI-08(02): AUTOMATIC UPDATES

Priority: P2	
Baseline(s): Moderate, High	Overlay(s): CMS-ARS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system automatically updates spam protection mechanisms.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
REFERENCES	**RELATED CONTROLS**
Federal: FedRAMP Rev. 4 Baseline; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.	

SI-10: INFORMATION INPUT VALIDATION

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system checks the validity of defined information inputs (defined in the applicable System Security Plan) for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. **CMS-ARS:** PII: The information system checks the validity of personally identifiable information (PII).	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std.1 - User input form fields need to be tested for malicious commands (e.g., SQL injection). Std.2 - Ensure user data is in the proper format before being accepted by the application. Std.3 - SQL queries should be crafted with user content passed into a bind variable and should avoid creation by dynamic string concatenation.	
SUPPLEMENTAL GUIDANCE	
Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks. PII: Information input validation serves two important purposes for protecting PII:	

(1) When PII is entered, validation techniques support data quality measures (e.g., ensuring the PII entered is the expected type and format of data); and (2) It provides the capability to limit or exclude PII from being entered into a field (e.g., recognizing a restricted format, such as an SSN).	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; IRS1075; CJIS 5.6	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Information system capability for checking validity of information inputs.	

SI-11: ERROR HANDLING

Priority: P2	
Baseline(s): Low Plus, Moderate, High	Overlay(s): Web & Mobile, DIR, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to defined personnel or roles (defined in the applicable System Security Plan). **CMS-ARS:** PII: The information system reveals error messages only to authorized individuals with a need for the information in the performance of their duties.	
CONTROL IMPLEMENTATION STANDARDS	
Web & Mobile: Std.1 - Error messages should not reveal details about the internal functionality of the application. Std.2 - Turn off debugging on production webservers. **CMS-ARS:** Std.1 - For cloud service providers, this Standard replaces the requirement defined within SI-11. The information system generates error messages that provide information necessary for corrective actions without revealing user name and password combinations; attributes used to validate a password reset request (e.g., security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings in error logs and administrative messages that could be exploited by adversaries.	
SUPPLEMENTAL GUIDANCE	
Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, Social Security Numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. PII:	

An error in a system may reveal sensitive information such as personally identifiable information (PII or protected health information (PHI). For example, if there is an error posting a form that contains PII and the system includes the PII entered in the form when it writes to the error log, it will be visible to whoever has access permissions to the error log. Therefore, error handling must be considered in design of the system, and access to errors containing leaked sensitive information should be provided only to those individuals with a need for that information in the performance of their duties.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: 5 U.S.C. §552a(e)(5) and (10); FedRAMP Rev. 4 Baseline; FISCAM: BP-1, BP-2, BP-3, BP-4, IN-1, IN-2; OMB Circular A-130: 7.g.; 45 C.F.R. §164.308(a)(3)(i); IRS1075; CJIS 5.6	AU-2, AU-3, SI-2
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Information system error handling capability.	

SI-12: INFORMATION HANDLING AND RETENTION

Priority: P2	
Baseline(s): Low, Low Plus, Moderate, High	Overlay(s): DIR, HIPAA, CMS-ARS, IRS, CJIS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	
CONTROL IMPLEMENTATION STANDARDS	
HIPAA: Std.1 - HIPAA requires that the following actions, activities, and assessments relating to the security of systems containing PHI be documented and retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later: a. Decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question; b. A user's right of access to a workstation, transaction, program, or process; c. Security incidents and their outcomes; d. Satisfactory assurances that a business associate will appropriately safeguard PHI. This documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements. If satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained; e. Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and f. Changes to organizational policies and procedures. **CMS-ARS:** Std.1 - Retain output, including but not limited to audit records, system reports, business and financial reports, and business records from the information system in accordance with CMS Policy and all applicable NARA requirements. **CMS-MARS-E:** Std.1 - The organization retains output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system for ten (10) years or in accordance with Administering Entity organizational requirements, whichever is more restrictive.	
SUPPLEMENTAL GUIDANCE	

Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. NARA provides guidance on records retention. PII: Sensitive information such as PII, even if not considered a "record" by statute, should be handled and retained in accordance with applicable regulatory requirements, organizational policies, industry best practices, and the Fair Information Practice Principles (FIPP). Retention and handling of PII that meets the definition of a "record" as defined by the Federal Records Act (44 U.S.C. §3301) should be addressed in a records disposition schedule. For PII that meets the definition of a "record" as defined by the Privacy Act for purposes of providing notice, the associated SORN should reflect the retention period from the organization's applicable record retention schedule. Protected health information (PHI) must be handled and retained in accordance with the HIPAA Security Rule as it has specific requirements for information handling and record retention.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** Code: U.S.C. §552a(e)(4); FedRAMP Rev. 4 Baseline; FISCAM: BP-3; 44 U.S.C. §3301, 45 C.F.R. §164.316(b)(1)(ii); 45 C.F.R. §164.316(b)(2)(i); IRS1075; CJIS 5.6	AC-16, AU-5, AU-11, MP-2, MP-4, AP-2, DM-2, TR-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records. Interview: Organizational personnel with information output handling and retention responsibilities.	

SI-16: MEMORY PROTECTION

Priority: P1	
Baseline(s): Low Plus, Moderate, High	Overlay(s): DIR, CMS-ARS, IRS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The information system implements security safeguards (e.g., data execution prevention, address space layout randomization) to protect its memory from unauthorized code execution. Implemented safeguards must be specified in the applicable System Security Plan.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can either be hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.	
REFERENCES	**RELATED CONTROLS**
Texas HHS: IS-Policy **State:** DIR Security Control Standards Catalog **Federal:** FedRAMP Rev. 4 Baseline; IRS1075	AC-25, SC-3
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: System and information integrity policy; system security plan; other relevant documents or records. Interview: Organizational personnel with information system development responsibilities.	

Appendix C: HHS Information Security and Privacy Controls

(AP) AUTHORITY AND PURPOSE

This family assists the Privacy Act compliance by ensuring that organizations: (i) identify the legal bases that authorize a particular Personally Identifiable Information (PII) collection or activity that impacts privacy; and (ii) specify the purpose(s) for which they collect PII in their notices.

AP-01: AUTHORITY TO COLLECT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of specific programs and the needs of information systems.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
An organization identifies the legal authority permitting collection. Additional measures, including design choices, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorities permitting the collection. Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the Senior Official for Privacy (SOP), and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements. Ensure PII collected, used, maintained, or disseminated by the information system is related to, and compatible with, the purpose and scope of the authority described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable. **CMS-MARS-E:** This standard ensures the organization identifies the legal bases that authorize a particular collection of PII, or activity that impacts privacy. The authorities to collect, use, maintain, and share PII must be clearly documented. When documentation appears in an agreement, citation(s) to the applicable law(s), regulation(s), and/or program guidance appear in an Authorities section of the agreement. Before collecting PII, the organization determines whether the contemplated collection of PII is legally authorized. Program officials consult with the designated privacy official and legal counsel regarding the authority of any program or activity to collect PII. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements (CMA). The organization may not create, collect, use, or disclose PII unless in compliance with 45 CFR §155.260. The CMA between the Centers for Medicare & Medicaid Services and State-based Administering Entities (AE) for the Disclosure of Insurance Affordability Programs Information under the Patient Protection and Affordable Care Act, establishes the terms, conditions, safeguards, and procedures under which CMS will disclose certain information to the AEs in accordance with the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act (Public Law 111-152), which are referred to collectively as the ACA, amendments to the Social Security Act made by the ACA, and the implementing regulations. Information Exchange Agreements (IEA) between CMS and AEs should also include the legal authority that permits the collection, use, maintenance, and sharing of PII. For Non-Federal Systems: The authority to collect, use, maintain, or disclose PII is based on ACA mandate for access to health insurance coverage, and/or based on state statute and regulations. The authority is	

documented in a PIA. The authority may also be included in other applicable documentation such as the CMS and IEAs as described.	
REFERENCES	**RELATED CONTROLS**
Code: 5 U.S.C. §552a, Pub. L. No. 107-347, §208; E-Gov: §208(c); OMB Circular A-130: Appendix I; Privacy Act: §552a(e)	AR-2, DM-1, TR-01, TR-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization determines the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need; and (ii) The organization documents the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Legal authority that permits the collection, use, maintenance, and sharing of PII; PII collection, use, maintenance, and sharing program policy; PII collection, use, maintenance, and sharing program procedures; other relevant documents or records. Examine: SORN and/or PIA and verify that the legal authority is stated.	

AP-02: PURPOSE SPECIFICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization, at the system or application level, describes the purpose(s) for which PII is collected, used, maintained, and shared in privacy compliance documentation and in its privacy notices (e.g., PIAs, SORNs, Privacy Act Statements, or CMAs).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
An organization identifies the authorized purpose(s) for collection, use, maintenance, or dissemination of PII. Additional measures, including, but not limited to, design choices and auditing, ensure the information system collecting, using, maintaining, or disseminating PII complies with those authorized purposes. Often, statutory language expressly authorizes specific collections and uses of PII. When statutory language is written broadly and thus subject to interpretation, organizations ensure, in consultation with the Senior Official for Privacy (SOP) and legal counsel, that there is a close nexus between the general authorization and any specific collection of PII. Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to PIAs, SORNs, and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). Further, in order to avoid unauthorized collections or uses of PII, personnel who handle PII receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice. Ensure the PII collected, used, maintained, or disseminated by the information system adheres to the specific purpose(s) described in the information system documentation, including privacy documentation such as a SORN or PIA when applicable.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(3)(A)-(B), Pub. L. No. 107-347, §208(b)(2)(B)(ii) and (c)(1)(B); E-Gov: §208(b), §208(c); Privacy Act: §552a(e)(3)(A)-(B)	AR-2, AR-4, AR-5, DM-1, DM-2, TR-01, TR-02, UL-01, UL-02
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization describes the purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices. Determine if: (i) The system only collects and uses PII relevant to its purposes; (ii) PII entering the system from other systems is limited to predetermined data elements; (iii) Generation of new PII is restricted to pre-determined data elements; (iv) PII output is properly labeled regarding permissible uses and restrictions on usage of the PII; (v) PII is only transferred to authorized entities for predetermined, documented purposes and business needs;	

(vi) When transferring PII to other agency systems or to third parties via the user interface, the system notifies the user of the permissible uses and restrictions on usage of the PII; (vii) User interfaces provide a notification when saving PII outside the system or printing PII, reminding the user of the permissible uses and restrictions on usage of the PII; and (viii) The system limits disclosure of PII to those data elements that are necessary for the purposes of the system.
ASSESSMENT METHODS AND OBJECTS
Examine: Privacy notice that describes the purpose for which PII can be collected, used, maintained, and shared; other relevant documents or records. Examine: System data model and database architecture and associate each PII data element or logical aggregate of elements (e.g., mailing address) with a rationale for its inclusion. Comment: Purpose Limitation is fundamentally system-specific. The implementation of this principle is heavily dependent on legal authorization and policy and could vary greatly for individual systems. Of the Enterprise Privacy Requirements, this is likely the most difficult for generating generic tests. Examine: User interfaces in which PII is entered. Establish rationale for any unstructured capture mechanisms (e.g., free text boxes). Comment: Structured mechanisms for capturing PII input (e.g., discrete and appropriately formatted input fields for specific PII data elements) help constrain the PII that can be captured. Examine: Display screens for evidence of appropriate warning. Comment: Unstructured data inputs pose a risk, as they are difficult to govern and users can enter any information they choose. Examine: Interfaces to verify PII data elements being requested. Comment: Individual queries may also be executed. Volume of queries may drive the approach used. Examine: Interfaces to verify PII data elements being received. Comment: May also send full record to system, including unnecessary PII data elements. Unnecessary PII data elements may also be sent individually; however, it is likely more efficient/feasible to send a record that contains multiple types of elements that should not be accepted. Examine: Output of each system function for PII data elements. Test: Attempt to save a file or data extract from the system that contains PII. Test: Attempt to print a file containing PII from the system. Comment: Notification may be handled in multiple ways, depending on the capabilities of the system, including screen views or pop-up notices. Test: Create and save a file containing system output with PII and review the label associated with it. Comment: This requirement depends on system capabilities. When available, automated means of applying labels should be used. Test: Print a file containing PII and review the label printed on it. Comment: Labels may include a file header or footer, a watermark, a designation in the file name, or some other means of communicating the authorized purpose. Test: Create and save a file containing system output with PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the authorized use. Comment: When practical for the purpose, consider making electronic file outputs read-only. Test: Submit a request to print a report containing PII. Attempt to alter the label that communicates the authorized use. Attempt to remove the label that communicates the authorized use. Examine: Interfaces to verify that PII is being transferred to the intended systems. Examine: Connection permissions for systems against the list of systems allowed to transfer PII out of the system. Test: Attempt to connect from an unauthorized system and transfer PII out of the system. Test: Attempt to initiate from system transfer of PII to an unauthorized system. Comment: Sharing agreements with third parties may include information documented in SORNs, information sharing agreements (ISA), memoranda of understanding (MOU), memoranda of agreement (MOA), and other formal agreements. Test: Attempt to transfer PII from the system and observe any notification provided. Comment: Notification may be handled in multiple ways, depending on the capabilities of the system, including screen views or pop-up notices. Depending on business requirements, the system may also be required to support an acknowledgement of notice received by the user. Examine: Target system updates to verify PII data elements being sent. Test: Attempt queries from target systems for PII data elements not pre-determined to be necessary. Comment: Additional thought may be required when full records are being disclosed, including whether disclosure of the full record (instead of specific data elements) is compatible with the purposes of the system.

AP-CMS-01: AUTHORITY AND PURPOSE CONTROL FAMILY POLICY AND PROCEDURE

Priority: P1

Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An Authority and Purpose policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Authority and Purpose policy and associated Authority and Purpose controls; and b. Reviews and updates (as necessary) the current: 1. Accountability, Audit, and Risk Management policy at least every two (2) years; and 2. Accountability, Audit, and Risk Management procedures at least every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: E-Gov: §208(b), §208(c); OMB Circular A-130: Appendix I; Privacy Act: §552a(e)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Authority to collect policy and procedures, and other relevant documents. Interview: Organizational personnel with authority to collect responsibilities, ensure responsibilities are acknowledged.	

(AR) ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

This family is intended to enhance public confidence through effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that an organization is complying with all applicable privacy protection requirements and minimizing its overall privacy risk.

AR-01: GOVERNANCE AND PRIVACY PROGRAM

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Appoints a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates an appropriate allocation of budget and staffing resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;	

e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and
f. Updates privacy plan, policies, and procedures, as required to address changing requirements, but no less often than every two years.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Development of the strategic organizational privacy plan must be done in consultation with the HHS CIO and CISO. The organization establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community:
(a) To facilitate ongoing privacy education and Technical Reference Architecture training for organizational personnel;
(b) To maintain currency with recommended privacy practices, techniques, and technologies; and
(c) To share current privacy-related information including threats, vulnerabilities, and incidents.

SUPPLEMENTAL GUIDANCE

Effective implementation of privacy and security controls requires a collaborative partnering of the SOP (or Chief Privacy Officer [CPO]), CIO, and CISO. To maximize organizational compliance with privacy requirements and best practices, the organization should ensure its privacy professionals engage with both its security community and the Federal privacy community to remain current and to share lessons-learned or other privacy-related information.

The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy. Accountability begins with the appointment of a SOP with the authority, mission, resources, and responsibility to develop and implement a multifaceted privacy program. The SOP, in consultation with legal counsel, information security officials, and others as appropriate: (i) ensures the development, implementation, and enforcement of privacy policies and procedures; (ii) defines roles and responsibilities for protecting PII; (iii) determines the level of information sensitivity with regard to PII holdings; (iv) identifies the laws, regulations, and internal policies that apply to the PII; (v) monitors privacy best practices; and (vi) monitors/audits compliance with identified privacy controls.

To further accountability, the SOP develops privacy plans to document the privacy requirements of organizations and the privacy and security controls in place or planned for meeting those requirements. The plan serves as evidence of organizational privacy operations and supports resource requests by the SOP. A single plan or multiple plans may be necessary depending upon the organizational structures, requirements, and resources, and the plan(s) may vary in comprehensiveness. For example, a one-page privacy plan may cover privacy policies, documentation, and controls already in place, such as Privacy Impact Assessments (PIA) and System of Records Notices (SORN). A comprehensive plan may include a baseline of privacy controls selected from this appendix and include: (i) processes for conducting privacy risk assessments; (ii) templates and guidance for completing PIAs and SORNs; (iii) privacy training and awareness requirements; (iv) requirements for contractors processing PII; (v) plans for eliminating unnecessary PII holdings; and (vi) a framework for measuring annual performance goals and objectives for implementing identified privacy controls.
Ongoing contact with privacy groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Privacy groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of privacy professionals in similar organizations.
Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

HIPAA:
HIPAA requires policies, procedures, and personnel designations to be documented and for organizations to monitor changes in law.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.530(a)(1)(i), 45 C.F.R. §164.530(i)(1), (2), and (3); Code: 44 U.S.C.: §3541, 5 U.S.C. §552a, 44 U.S.C. §3506 (a)(3) and (g), Pub. L. No. 107-347, §208; OMB Memo: M-03-22, M-05-08, M-07-16; OMB Circular A-130:; Privacy Act: §552a	AP-CMS-01, AR-CMS-01, DI-CMS-01, DM-CMS-01, IP-CMS-01, TR-CMS-01, UL-CMS-01, PM-15

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:

(i) The organization appoints a Senior Official for Privacy (SOP) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems; (ii) The organization monitors federal privacy laws and policy for changes that affect the privacy program; (iii) The organization allocates an appropriate allocation of budget and staffing to implement and operate the organization-wide privacy program; (iv) The organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; (v) The organization develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and (vi) The organization updates privacy plan, policies, and procedures, as required to address changing requirements, but at least every two years.
ASSESSMENT METHODS AND OBJECTS
Examine: Organizational governance and privacy policy; governance and privacy program plan; governance and privacy procedures; budget and staffing documentation; strategic organizational privacy plan; privacy policies and procedures; information system privacy and security controls; other relevant documents or records. Interview: Organizational person appointed to the senior privacy officer/official position.

AR-02: PRIVACY IMPACT AND RISK ASSESSMENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII; b. Conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures; and **CMS-ARS:** c. Reviews the PIA no less than every three (3) years and publishes the PIA in accordance with HHS guidance.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Effective implementation of privacy risk management processes requires both organizational and information system processes across the life cycle of the mission, business processes, and information system. Privacy Impact Assessments are structured reviews (qualitative and quantitative) of both the risk and effect of how information is handled and maintained as well as the potential impacts or harms to individuals and organizations for loss of control or mishandling of the PII.34 A PIA-like process, even if not required for a particular information system, benefits an organization and the individuals whose PII is in the information system by enabling the organization to identify, evaluate, and manage the privacy risks for the PII in that system. Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems. Some organizations may be required by law or policy to extend the PIA requirement to other activities involving PII or otherwise impacting privacy (e.g., programs, projects, or regulations). PIAs are conducted to identify privacy risks and identify methods to mitigate those risks. PIAs are also conducted to ensure that programs or information systems comply with legal, regulatory, and policy requirements. PIAs also serve as notice to the public of privacy practices. PIAs are performed before developing or procuring information systems, or initiating programs or projects, that collect, use, maintain, or share PII and are updated when changes create new privacy risks. Information system privacy risk management processes operate across the life cycle of an information system collecting, using, maintaining, and/or disseminating PII. Such privacy risk management processes include, but are not limited to, design requirements, privacy threshold analysis, privacy impact assessments (PIA), and implementation of secure disposition. While Section 208 of the E-Government Act does not require — or prohibit	

— a PIA for a national security system (NSS), as defined at 40 U.S.C. §11103 (see Section 202(i) of the E-Government Act), an organization may benefit from conducting a PIA or similar privacy risk evaluation on NSS as part of their internal risk management process to ensure privacy risks are identified, evaluated, and managed in information systems containing PII.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.530(c); Code: 44 U.S.C.: §3541; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-10-23; OMB Circular A-130: 7.g., 8.a.(1), 8.b.(2), and 8.b.(3)	RA-3

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing,
transmitting, use, and disposal of PII; and
(ii) The organization conducts PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.
Determine if the Privacy controls and protection of PII have been considered in the ISRA.
Determine if:
(i) The system's security controls are based on a confidentiality impact level equal to or greater than the PII confidentiality impact level.

ASSESSMENT METHODS AND OBJECTS

Examine: Privacy risk management planning policy; procedures addressing privacy impact assessments on the information system; privacy impact assessment; other relevant documents or records.
Interview: Interview the Information System Security Officer (ISSO) and/or the Information Owner(s)/Custodian(s) to determine if the Privacy controls and protection of PII have been considered in their information security risk assessment (ISRA). Ensure the organization has a finalized privacy impact assessment (PIA) that has been signed within the last three years.
Examine: PII and system confidentiality impact levels and compare the two.
Examine: Final PIA and confirm that PIA is published on HHS website.

AR-03: PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers;
b. Includes privacy requirements in contracts and other acquisition-related documents; and
c. Reviews, every two (2) years, a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the contracts include clauses that make all requirements of the Privacy Act apply to the system and that make the criminal penalty provisions of the Privacy Act apply to the contractor or service provider and its personnel.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - The contract or other acquisition-related documents must flow-down privacy and security clauses to ensure sub-contractors adequately protect personally identifiable information (PII).

HIPAA:
Std.2 - Under HIPAA, a business associate must ensure its contracts or other arrangements with subcontractors meet the requirements of 45 §C.F.R. §164.504(e).

SUPPLEMENTAL GUIDANCE

Contracts and other acquisition-related documents provide an enforceable means to ensure privacy and security controls follow the information, and that contractors and service providers protect PII in the same way the organization does.

Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Official for Privacy (SOP), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the SOP, and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.

CMS-MARS-E:
Specific to Non-Exchange Entities (NEE): Regulatory provisions at 45 CFR §155.260 describe how Marketplace privacy and security requirements apply to non-Exchange entities (NEE). 45 CFR §155.260(b)(1) defines NEEs as any individual or entity that: (i) gains access to personally identifiable information submitted to an Exchange; or (ii) collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.

Specific to Marketplaces: §155.260(b)(2) requires that, before any person or entity becomes a NEE, the Marketplace must execute with that person or entity a contract or agreement that includes provisions that are specified at §155.260(b)(2)(i)-(v). These provisions must:
1. Describe the functions the NEE is to perform;
2. Bind the NEE to comply with privacy and security requirements adopted in accordance with paragraph §155.260(b)(3), specifically listing or incorporating those privacy and security standards and obligations;
3. Require the NEE to monitor, periodically assess, and update its security controls and related system risk to ensure their continued effectiveness;
4. Require the NEE to inform the Marketplace of any changes in its administrative, technical, or operational environments defined as material within the contract; and
5. Require the NEE to bind any downstream entities to the same privacy and security standards and obligations to which the NEE has agreed in its contract or agreement with the Marketplace

§155.260(b)(3) further requires that, when collection, use, or disclosure is not otherwise required by law, the privacy and security standards to which a Marketplace binds a NEE must be consistent with the principles and requirements listed in §155.260(a)(1)-(6), including, but not limited to, being at least as protective as the standards the Marketplace has established and implemented for itself in compliance with §155.260(a)(3). The standards to which a Marketplace binds a NEE also must adhere to the requirements listed at §155.260(c),(d),(f), and (g), and must take into specific consideration:

1. The environment in which the NEE operates;
2. Whether the standards are relevant and applicable to the NEE's duties and actives in connection with the Marketplace, and
3. Any existing legal requirements to which the NEE is bound in relation to its administrative, technical, and operational controls and practices, including, but not limited to, its existing data handling and information technology processes and protocols.

Specific to Medicaid and CHIP: While Medicaid/CHIP is itself an NEE, the organization must follow the guidance in §155.260(b)(2) stated above when executing an agreement with another NEE in performing a function for the Medicaid/CHIP agency.

REFERENCES	RELATED CONTROLS
Federal: CFR: 48 C.F.R. Part 24.102, 48 C.F.R. Part 39.105, 45 C.F.R. §164.504(e); 45 C.F.R. §164.530(c); Code: 5 U.S.C. §552a(m); FAR: Part 24; OMB Circular A-130: 7.g.; Privacy Act: §552a(m)	AR-1, AR-5, SA-4

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers;
(ii) The organization includes privacy requirements in contracts and other acquisition-related documents; and
(iii) The organization has documented procedures regarding privacy requirements for contractors or service providers and are implemented as described.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization privacy policy establishing privacy roles, responsibilities, and access requirements for contractors and service providers; privacy requirements in contracts and other acquisition-related documents; other relevant documents or records.

AR-04: PRIVACY MONITORING AND AUDITING

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization
a. Monitors and audits privacy controls no less often than once every 365 days to ensure effective implementation; and
b. Monitors for changes to applicable privacy laws, regulations, and policy affecting internal privacy policy no less often than once every 365 days to ensure internal privacy
policy remains effective; and

CMS-MARS-E:
c. Documents, tracks, and ensures mitigation of corrective actions identified through monitoring or auditing.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Monitoring and auditing activities ensure privacy controls are implemented and operating effectively. To promote accountability, organizations identify and address gaps in privacy compliance, management, operational, and technical controls by conducting regular assessments (e.g., internal risk assessments). These assessments can be self-assessments or third-party audits that result in reports on compliance gaps identified in programs, projects, and information systems. In addition to auditing for effective implementation of all privacy controls identified in [800-53 Appendix J], organizations assess whether they: (i) implement a process to embed privacy considerations into the life cycle of personally identifiable information (PII), programs, information systems, mission/business processes, and technology; (ii) monitor for changes to applicable privacy laws, regulations, and policies; (iii) track programs, information systems, and applications that collect and maintain PII to ensure compliance; (iv) ensure that access to PII is only on a need-to-know basis; and (v) ensure that PII is being maintained and used only for the legally authorized purposes identified in the public notice(s).
Organizations also: (i) implement technology to audit for the security, appropriate use, and loss of PII; (ii) perform reviews to ensure physical security of documents containing PII; (iii) assess contractor compliance with privacy requirements; and (iv) ensure that corrective actions identified as part of the assessment process are tracked and monitored until audit findings are corrected. The Senior Official for Privacy (SOP) coordinates monitoring and auditing efforts with information security officials and ensures that the results are provided to senior managers and oversight officials.

As many of the controls assigned by the Privacy Overlays are security controls, it is most efficient to develop a coordinated organizational process to conduct monitoring and audit. Where security and privacy controls align, in order to achieve the most efficient and effective implementation, the CMS SOP/CPO and CIO or CISO should coordinate to develop a single organizational process to conduct audit and monitoring.

REFERENCES	RELATED CONTROLS
Federal: Code: 44 U.S.C.: §3541; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-06-16, M-07-16; OMB Circular A-130:; Privacy Act: §552a; 45 C.F.R. §164.530(a)(1)(ii)	AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-01, UL-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization monitors and audits privacy controls and internal privacy policy as required to confirm effective implementation.
Determine if the system captures all requests to update personally identifiable information (PII) in the system and when the update has been completed
Determine if the system is equipped with mechanisms to produce trend and comparative analysis on the manipulation of PII, for systems that generate their own analysis of PII.
Determine if the system reports on inappropriate manipulation of PII.
Determine if the system recognizes established thresholds that when met signify suspicious user activity.
Determine if the system notifies the user, administrator, or other relevant party of any failure during transfer of PII.
Determine if the system maintains an audit log of attempts to produce new PII.
Determine if the organization tracks the storage and access of PII.
Determine if the PII is restricted to “need to know” and removed when no longer required.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization privacy policy monitoring and auditing requirements; internal privacy policy to confirm effective privacy control implementation; procedures for monitoring and auditing privacy controls; audit controls and records; other relevant documents or records. Examine: Review audit log that provides evidence of PII being updated in the system to verify its existence. Test: Submit updated test PII to the system. Test: Attempt to generate report on the total number of times updated PII was submitted to the system and the data fields updated within a specified time period. Comment: Comparative analysis may include frequency of requests to and action of updating PII, common data fields updated, and peak periods for these occurrences. Examine: Review function that generates trend and comparative analysis on newly produced or input PII. Comment: If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant. Examine: Review the system's design documentation for reporting function for system anomalies. Examine: Review the system's design documentation for analysis function. Test: Attempt to engage in a behavior (e.g., user excessively accessing records) that might indicate inappropriate use of PII. Test: Initiate a data transfer to an authorized system and introduce an interruption that will cause the transfer to fail. Observe any alerts produced by the system. Comment: Transfer failures can result in incomplete records for individuals. Examples of failures to introduce would be to disconnect one of the test systems from the network, attempt to connect to a destination system that will not allow a connection from the system being tested, or writing to a full drive. Notifications may include on-screen alerts, log entries, or some other method. Examine: Review audit log that shows evidence of new PII produced. Comment: If the system interface is highly constrained, where users and their degrees of freedom are predetermined, then technically this requirement should be a non-issue. Conversely, if users' freedoms are not predetermined and less controlled, then this requirement becomes more relevant. Interview: Interview the Information System Security Officer (ISSO)/Privacy Officer to determine how the organization tracks the storage and access of PII. Examine: Request and examine documentation describing the lifecycle of collected PII to determine if the PII is restricted to "need to know" and removed when no longer required. Examine: Examine any physical documents containing PII, and review records of monitoring and disposition.

AR-05: PRIVACY AWARENESS AND TRAINING

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops, implements, and updates a comprehensive privacy training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training no less often than once every three hundred sixty-five (365) days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII no less often than once every three hundred sixty-five (365) days; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements no less often than once every three hundred sixty-five (365) days.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 – A privacy education and awareness training program must be developed and implemented for all employees and individuals working on behalf of CMS involved in managing, using, and/or processing PII. Std.2 - Privacy education and awareness training must include responsibilities associated with sending PII in email. Std.3 - Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. Std.4 - Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to organization information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Std.5 - Additional or advanced training must be provided commensurate with increased responsibilities or change in duties. Std.6 - Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed.	

Std.7 - Training must address the rules for telework and other authorized remote access programs.	
SUPPLEMENTAL GUIDANCE	
Privacy Training is an effective means to reduce privacy risk for an organization and is mandated by the Privacy Act of 1974, as amended, and OMB M-07-16. Through implementation of a privacy training and awareness strategy, the organization promotes a culture of privacy. Privacy training and awareness programs typically focus on broad topics, such as responsibilities under the Privacy Act of 1974 and E-Government Act of 2002 and the consequences of failing to carry out those responsibilities, how to identify new privacy risks, how to mitigate privacy risks, and how and when to report privacy incidents. Privacy training may also target data collection and use requirements identified in public notices, such as Privacy Impact Assessments (PIA) or System of Records Notices (SORN) for a program or information system. Specific training methods may include: (i) mandatory annual privacy awareness training; (ii) targeted, role-based training; (iii) internal privacy program websites; (iv) manuals, guides, and handbooks; (v) slide presentations; (vi) events (e.g., privacy awareness week, privacy clean-up day); (vii) posters and brochures; and (viii) email messages to all employees and contractors. Organizations update training based on changing statutory, regulatory, mission, program, business process, and information system requirements, or on the results of compliance monitoring and auditing. Where appropriate, organizations may provide privacy training as part of existing information security training. Privacy training may be integrated with general IA training. Examples of jobs or roles that would require job-specific privacy and security training include: human resource personnel who have greater access to PII; system developers who design, develop and implement information systems containing PII; and system administrators who operate and maintain information systems containing PII. References: HHS IRM Policy for IT Security for Remote Access Master Labor Agreement	
REFERENCES	**RELATED CONTROLS**
Federal: Telework Enhancement Act of 2010; CFR: 45 C.F.R. §164.530(b)(1), 45 C.F.R. §164.530(a)(1)(ii); Code: 5 U.S.C. §552a(e)(9), 44 U.S.C.: §3541, Pub. L. No. 107-347, §208, Pub. L. No. 107-347, Title III; E-Gov: §208; OMB Memo: M-03-22, M-05-08, M-06-16, M-07-16, Att. 1, A.2.d.; OMB Circular A-130:; Privacy Act: §552a(e)	AR-3, AT-2, AT-3, TR-01
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; (ii) The organization administers basic privacy training at least every 365 days, and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at least every 365 days; (iii) The organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least every 365 days; and (iv) The organization meets all the requirements specified in the applicable Implementation Standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Training and awareness policy; training and awareness program plan strategy; privacy and awareness training material; training records; other relevant documents or records. Examine: Privacy role-based training and compliance tracking mechanisms. Interview: Organizational personnel with privacy training responsibilities. Interview: A sample of system users.	

AR-06: PRIVACY REPORTING

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization develops, disseminates, and updates reports to OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - HHS Information Security provides oversight of information security and privacy, to include privacy reporting, for each FISMA System operating by or on behalf of CMS.	
SUPPLEMENTAL GUIDANCE	

Privacy reporting helps organizations to determine progress in meeting privacy compliance requirements and to ensure organizational accountability. Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations determine progress in meeting privacy compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models. Types of privacy reports include: (i) annual Senior Official for Privacy (SOP) reports to OMB; (ii) reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; or (iii) other public reports required by specific statutory mandates or internal policies of organizations. The SOP consults with legal counsel, where appropriate, to ensure that organizations meet all applicable privacy reporting requirements.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §160.310(a); 45 C.F.R. §164.408; Code: 5 U.S.C. §552a, 44 U.S.C. §3541(4), 44 U.S.C. §3541, Pub. L. No. 107-347, §208; 9/11 Communication Act: §2000ee-1, Section 803, §2000ee-3, Section 804; Consolidated Appropriations Act: §522; E-Gov: §208; OMB Memo: M-08-09; OMB Circular A-130: 7.g.; Privacy Act: §552a	

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

PII:
Determine if:
(i) The organization develops privacy reports to OMB, Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory
privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance;
(ii) The organization disseminates privacy reports to the OMB, Congress, and other oversight bodies, as appropriate, and to senior management and other personnel with
responsibility for monitoring privacy program progress and compliance;
(iii) The organization updates privacy reports within the time period specified by specific statutory and regulatory privacy program mandates but no less than within every three
hundred sixty-five (365) days; and
(iv) The organization meets all the requirements specified in the applicable Implementation Standard(s).

ASSESSMENT METHODS AND OBJECTS

PII:
Examine: Reports to OMB, Congress, and other oversight bodies, as appropriate; reports to senior management and personnel with responsibility for monitoring privacy program progress and compliance; other relevant documents or records.
Interview: Organizational personnel with information security and privacy responsibilities.

AR-07: PRIVACY-ENHANCED SYSTEM DESIGN AND DEPLOYMENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization designs information systems to support privacy by automating privacy controls to the extent feasible, integrating and meeting privacy requirements throughout the CMS Life Cycle, and incorporating privacy concerns into reviews of significant changes to HHS/CMS systems, networks, physical environments, and other agency infrastructures.

The organization also conducts periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act, the organization's privacy policy, and any other legal or regulatory requirements.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Automating privacy controls provides a concrete way of ensuring information systems are behaving in a way that is intended to achieve privacy objectives. Implementation of this Privacy Overlay enables organizations to automate application of privacy controls. One simple example, which many organizations have already implemented, is TR-01, "Privacy Notice." This concept is one part of the most commonly recognized approach to "building privacy in" which is "Privacy by Design." Privacy by Design is an internationally accepted privacy best practice endorsed by the Federal Trade Commission in their March 2012 Final Report, Protecting Consumer Privacy in an Era of Rapid Change:

Recommendations for Businesses and Policymakers, and embodies the same principles of the Privacy Act and Section 208 of the E-Government Act requiring privacy protections and safeguards before establishing or operating a system that may contain PII. Privacy by Design calls for considering privacy risks in the design and management of information systems. In addition to building in security and privacy controls discussed throughout this overlay, this control considers additional privacy-specific system characteristics and controls that must be built into the system to address privacy risks.

To the extent feasible, when designing organizational information systems, organizations employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of personally identifiable information (PII). By building privacy controls into system design and development, organizations mitigate privacy risks to PII, thereby reducing the likelihood of information system breaches and other privacy-related incidents. Organizations also conduct periodic reviews of systems to determine the need for updates to maintain compliance with the Privacy Act and the organization's privacy policy.
Regardless of whether automated privacy controls are employed, organizations regularly monitor information system use and sharing of PII to ensure that the use/sharing is consistent with the authorized purposes identified in the Privacy Act and/or in the public notice of organizations, or in a manner compatible with those purposes.

Additional guidance on privacy-enhanced design and development found in the HHS EPLC. Regardless of the systems engineering lifecycle used, privacy requirements should be considered during system design and development and validated and verified along with other system requirements. Validation ensures the correct requirements were identified. Verification ensures the requirements were implemented correctly.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.530(c); Code: 5 U.S.C. §552a, Pub. L. No. 107-347, §208; E-Gov: §208(b), §208(c); OMB Memo: M-03-22, M-07-16; OMB Reports: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Federal Trade Commission Final Report (March 2012); Privacy Act: §552a(e)(10)	AC-6, AR-4, AR-5, DM-2, TR-01, SA-3, SA-8

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

PII:
Determine if the organization designs information systems to support privacy by automating privacy controls.
Determine if:
(i) The system's technical monitoring and reporting functionalities are consistent with those described in the system's privacy compliance documents;
(ii) PII data fields are properly tagged as PII, for systems with supporting technology;
(iii) PII transferred to other systems is transferred with proper tagging of data fields, for systems with supporting technology; and
(iv) Views of PII are defined for each distinct user and/or target system role.

ASSESSMENT METHODS AND OBJECTS

PII:
Examine: Information system design documentation; other relevant documents or records.
Examine: The application of technical monitoring and reporting functionalities in the system to confirm that they match technical functionalities described in the system's privacy impact assessment (PIA), system of records notice (SORN), and any other privacy compliance documents that describe this information.
Examine: Database schema to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.
Examine: Data fields within the database to confirm that PII data elements are tagged as such and that other data elements are not tagged as PII.
Test: Attempt to transfer data to an authorized system. Review the manner in which the target system handles the data field tags for PII. Comment: This test is outside the boundary of the system tested; however, it is a critical step in the use of data tagging and must be considered. Metadata should be included in this review and may be the primary means for meeting this requirement. Metadata may provide information such as time/date stamps, purposes of the PII, and other valuable information about the data.
Examine: System design documentation to view template design.
Test: Logon to the system as test users with differing roles to verify that viewable PII is consistent with roles.
Test: Log into the system as test users with differing roles to verify that views are consistent with roles
Examine: System functions used to generate reports.
Examine: Access controls for user accounts and target system connections.

AR-08: ACCOUNTING OF DISCLOSURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
(1) Date, nature, and purpose of each disclosure of a record; and
(2) Name and address of the person or agency to which the disclosure was made.
b. Retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer; and
c. Makes the accounting of disclosures available to the person named in the record upon request.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Both the Privacy Act and HIPAA require accounting of disclosures in certain circumstances. There are differences in the requirements to account for disclosures under the Privacy Act and under HIPAA.
The Senior Official for Privacy (SOP), periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act. Organizations are not required to keep an accounting of disclosures when the disclosures are made to individuals with a need to know, are made pursuant to the Freedom of Information Act, or are made to a law enforcement agency pursuant to 5 U.S.C. §552a(c)(3). Heads of agencies can promulgate rules to exempt certain systems of records from the requirement to provide the accounting of disclosures to individuals.

HIPAA:
HIPAA covered entities have specific accounting of disclosure requirements. An accounting of disclosure documents the disclosures of PHI made by the organization to third parties. Not all disclosures are required to be reported, for specific accounting disclosure requirements see 45 C.F.R. §164.528.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.528; Code: 5 U.S.C. §552a(c), (j), and (k); Privacy Act: §552a(c)(1), §552a(c)(3), §552a(j), §552a(k)	IP-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
a. The organization retains the accounting of disclosures for the life of the record or five (5) years after the disclosure is made, whichever is longer; and
b. The organization makes the accounting of disclosures available to the person named in the record upon request.
Determine if:
(i) Personally identifiable information (PII) exchanges between the system and third parties are accounted for by formal documentation (e.g., privacy impact assessment [PIA],
memorandum of understanding [MOU], information sharing agreement [ISA]); and
(ii) The system logs the date, purpose, and to whom the record was disclosed, for systems that maintain an accounting of disclosures under sub-section (c) of the Privacy Act.

ASSESSMENT METHODS AND OBJECTS

Examine: Records documenting the disclosures of information held in each system of records under its control; retention policy for the disclosure records; policy for making the disclosures available to the person named in the record upon request; other relevant documents or records.
Interview: Interview the Information System Security Officer (ISSO) and/or Information Owner(s)/Custodian(s) to ensure they are recording disclosure of privacy information if it occurs. Request to view records of the disclosures, as appropriate.
Examine: Alignment between authorized system connections and system interface configurations to ensure that the system is interfacing only with authorized third party systems.
Examine: Applicable authorization agreement(s) against PII exchanges between the system and third parties to verify that data exchanges are authorized.

Examine: The system's design documentation to verify there is a function responsible for capturing information pertaining to disclosure activity. Test: Disclose PII from the system to a target entity to verify that the disclosure is logged. Comment: Subsection (c) of the Privacy Act requires the agency to keep accurate account of when and to whom it has disclosed PII. This includes the date, nature, and purpose of each disclosure of a record.

AR-CMS-01: ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT CONTROL FAMILY POLICY AND PROCEDURE

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS//
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. An Accountability, Audit, and Risk Management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Accountability, Audit, and Risk Management policy and associated Accountability, Audit, and Risk Management controls. b. Reviews and updates (as necessary) the current: 1. Accountability, Audit, and Risk Management policy at least every two (2) years or when there has been a significant change in applicable privacy laws, regulations, and policy affecting internal privacy policy; and 2. Accountability, Audit, and Risk Management procedures at least every two (2) years or when there has been a significant change in applicable privacy laws, regulations, and policy affecting internal privacy policy.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - The SSP must document this control family. If the system does not contain PII or PHI, the controls within this family must be documented as "Limited Applicability - System does not process PII nor PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 44 U.S.C.: §3541; E-Gov:: §208; FAR: Part 24; OMB Memo: M-03-22, M-05-08, M-06-16, M-07-16, M-10-23; OMB Circular A-130:; Privacy Act: §552a	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Accountability, audit, and risk management policy and procedures, and other relevant documents. Interview: Organizational personnel with accountability, audit, and risk management responsibilities, ensure responsibilities are acknowledged.	

(DI) DATA QUALITY AND INTEGRITY

This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the public notice.

DI-01: DATA QUALITY

Priority: P1

Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
b. Collects PII directly from the individual to the greatest extent practicable;
c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems no less often than once every 365 days or as directed by the Data Integrity Board; and
d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

When a record is used to make a determination of a right, benefit, or privilege for an individual, the Privacy Act of 1974, as amended, requires the information used be accurate, relevant, timely, and complete to assure fairness to the individual in the determination. Agencies should ensure the quality of all of its PII, even if it is not protected by the Privacy Act. Organization's data quality assurance process should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

Organizations take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, for example, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs may be more comprehensive than those used to validate less sensitive PII. Additional steps may be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals. When PII is of a sufficiently sensitive nature (e.g., a patient's health data), organizations incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations should incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be confirmed accurate, relevant, timely, and complete. Frequency of confirmation should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office.

REFERENCES	RELATED CONTROLS
Federal: 5 U.S.C. §552a(e)(5;); OMB Memo: M-07-16; OMB Circular A-130: Appendix I, 7.g. and 8.a.9; Paperwork Reduction Act, 44 U.S.C. §3501; Privacy Act: §552a(c), §552a(e), §552a(a)(8)(A), §552a(o), §552a(p), §552a(u); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C §515, 114 Stat. 2763A-153-4	AP-2, DI-2, DM-1, IP-03, SI-10

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization confirms to the greatest extent practicable upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
(ii) The organization collects PII directly from the individual to the greatest extent practicable;
(iii) The organization checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems as directed by the Data Integrity Board; and
(iv) The organization issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.
Determine if:
(i) The system ensures that multiple instances of the same PII data elements do not deviate unacceptably in their values;
(ii) The system checks time sequenced PII to ensure correct sequencing;
(iii) The system checks received PII for type and format consistency;
(iv) The system checks PII date thresholds to detect outdated PII and alert the user;

(v) The system recognizes and alerts the user when PII is not sufficiently complete to adequately accomplish the intended purposes of the system; and (vi) PII collected directly from the individual takes precedence over PII collected from third parties.
ASSESSMENT METHODS AND OBJECTS
Examine: Organization privacy policy; privacy program plan; privacy program procedures; guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information; other relevant documents or records. Examine: All instances where the test PII data elements appear in the system. Test: Enter incorrectly sequenced PII into the system and observe any warnings provided. Comment: The exact nature of what is tested is highly system dependent. Test: Submit a numeric value for an alphabetic field and an alphabetic value for a numeric field. Test: Submit an alpha-numeric PII element to the system that is incompatible with the length or format expected. Test: Submit test PII that is not logically consistent (e.g., date of birth [DoB] and age do not match) to the system and observe any warnings. Comment: The exact nature of what is tested is highly system dependent. Test: Submit test PII to the system that is out of date for the intended purposes and observe any warnings. Test: Submit test PII that does not meet the established level of completeness to the system and observe any warnings. Comment: The exact nature of what is tested is highly system dependent. Test: Submit test PII collected as a third party source and the same test PII collected from the individual to the system with variations in the two PII submissions. Comment: Applies to systems where similar PII element(s) gathered from both the individual and one or more third party sources are collected, processed, or propagated, and where the PII from either source may be used to accomplish the purposes of the system.

DI-01(01): VALIDATE PII

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization requests that the individual or individual's authorized representative validate PII during the collection process.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Validating PII, used to determine a right, benefit, or privilege for an individual, ensures the determination is based on accurate, timely, and relevant information. Procedures for validating PII should be commensurate with the impact to an individual's rights, benefits, or privileges as determined by the system owner in consultation with the organization's privacy office. When PII is of a sufficiently sensitive nature (such as, but not limited to, when it is used for annual reconfirmation of a taxpayer's income for a recurring benefit or adjudication of an employee's clearance), organizations incorporate mechanisms into information systems and develop corresponding procedures and methods to validate the PII is accurate, relevant, timely, and complete.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(5;); OMB Circular A-130: 7.g. and 8.a.9.	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization requests that the individual or individual's authorized representative validate PII during the collection process.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Organization privacy policy; privacy program plan; privacy program procedures; PII validation procedures; other relevant documents or records.	

DI-02: DATA INTEGRITY AND DATA INTEGRITY BOARD

Priority:	
Baseline(s):	Overlay(s): CMS-MARS-E, VA
CONTROL REQUIREMENTS	
Non-Federal entities are not required to implement this control	

a. The organization document processes and procedures to ensure the integrity of PII through existing security controls. b. The organization establishes a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
Organizations conducting or participating in CMAs with other organizations regarding applicants for and recipients of financial assistance or payments under Federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the designated privacy official. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs.

REFERENCES	RELATED CONTROLS
	AC-1, AC-3, AC-4, AC-6, AC-17, AC-22, AU-2, AU-3, AU-6, AU-10, AU-11, DI-1, SC-8, SC-28, UL-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if: 1. The organization documents processes to ensure the integrity of PII through existing security controls; and 2. The organization establishes a Data Integrity Board when appropriate to oversee organizational CMAs and to ensure those agreements comply with the computer matching provisions of the Privacy Act.
ASSESSMENT METHODS AND OBJECTS
Examine: Organization PII integrity policy; PII integrity program plan; PII integrity process and procedures; information security plan; other relevant documents or records.

DI-02(01): PUBLISH AGREEMENTS ON WEBSITE

Priority:	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
Non-Federal entities are not required to implement this control The organization publishes CMA's on its public website	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Organizations conducting or participating in CMAs with other organizations regarding applicants for and recipients of financial assistance or payments under Federal benefit programs or regarding certain computerized comparisons involving federal personnel or payroll records establish a Data Integrity Board to oversee and coordinate their implementation of such matching agreements. In many organizations, the Data Integrity Board is led by the designated privacy official. The Data Integrity Board ensures that controls are in place to maintain both the quality and the integrity of data shared under CMAs.	

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if CMS publishes CMAs for the FFM on its public website.
ASSESSMENT METHODS AND OBJECTS
Examine: Organization CMAs; other relevant documents or records.

DI-CMS-01: DATA QUALITY AND INTEGRITY CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. Data Quality and Integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Data Quality and Integrity policy and associated Data Quality and Integrity controls; and b. Reviews and updates (as necessary) the current: 1. Data Quality and Integrity policy within every two (2) years; and 2. Data Quality and Integrity procedures within every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII no PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the DI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: OMB Memo: M-07-16; OMB Circular A-130: Appendix I; Paperwork Reduction Act, 44 U.S.C. §3501; Privacy Act: §552a(c), §552a(e), §552a(a)(8)(A), §552a(o), §552a(p), §552a(u); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C §515, 114 Stat. 2763A-153-4	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Data quality and integrity policy and procedures, and other relevant documents. Interview: Organizational personnel with data quality and integrity responsibilities to ensure responsibilities are acknowledged.	

(DM) DATA MINIMIZATION AND RETENTION

This family assists organizations in implementing the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a NARA-approved record retention schedule.

DM-01: MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Identifies the minimum PII elements that are relevant and necessary to accomplish the purpose of collection (and where a collection of certain PII requires legal authorization, HHS/CMS must ensure that such collection is legally authorized); b. Limits the collection and retention of PII to the minimum elements identified in the notice and, when the collection of PII is made directly from the subject individual, limits its purposes to those for which the individual has provided consent to the extent permitted by law; and	

c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, no less often than once every three hundred sixty five (365) days, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Coordinating review of the organization's holdings of PII with existing system review processes maximizes the efficient use of organization resources and will ensure all PII retained, even if the PII is not maintained in a Privacy Act system of records, is relevant and accurate. Reducing PII to the minimum required to accomplish the legally authorized purpose of collection and retaining PII for the minimum necessary period of time reduces the risk of PII breaches and will reduce the risk of the organization making decisions based on inaccurate PII. Organizations take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect. Program officials and program representatives such as Data Guardians consult with the Senior Official for Privacy (SOP) and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

Organizations can further reduce their privacy and security risks by also reducing their inventory of PII, where appropriate. OMB Memorandum 07-16 requires organizations to conduct both an initial review and subsequent reviews of their holdings of all PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete. Organizations are also directed by OMB to reduce their holdings to the minimum necessary for the proper performance of a documented organizational business purpose. OMB Memorandum 07-16 requires organizations to develop and publicize, either through a notice in the Federal Register or on their websites, a schedule for periodic reviews of their holdings to supplement the initial review. Organizations coordinate with their federal records officers to ensure that reductions in organizational holdings of PII are consistent with NARA retention schedules.
Organizations should coordinate the PII holdings reviews with the systems' annual information security reviews schedule to the maximum extent practicable. By performing periodic evaluations, organizations reduce risk, ensure that they are collecting only the data specified in the notice, and ensure that the data collected is still relevant and necessary for the purpose(s) specified in the notice.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.502(b); Code: 5 U.S.C. §552a(e)(1); E-Gov: §208(b); OMB Memo: M-03-22, M-07-16; OMB Circular A-130: 7.g. and 8.a.; Privacy Act: §552a(e)	AP-1, AP-2, AR-4, IP-01, SE-01, SI-12, TR-01

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;
(ii) The organization limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent;
(iii) The organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings, at least every 365 days, to confirm that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
Determine if the system's intake of PII is consistent with the privacy notices related to the system, including System of Records Notice (SORN), Privacy Impact Assessment (PIA), and notices provided at points of collection.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization privacy data minimization and retention policy; privacy data minimization and retention program plan; privacy data minimization and retention program procedures; PII holding evaluation and review documentation; other relevant documents or records.
Examine: Documented system inputs with relevant privacy notices. Comment: Types and breadth of notice provided may vary widely by system. Testers must consult with relevant offices to confirm an accurate understanding of notice statements.

DM-01(01): MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-MARS-E
CONTROL REQUIREMENTS	
The organization, where feasible and within the limits of technology, locates, and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
NIST SP 800-122 provides guidance on anonymization	
REFERENCES	**RELATED CONTROLS**
Federal: NIST SP 800-122	AP-1, AP-2, AR-4, IP-01, SE-01, SI-12, TR-01
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Organization privacy data anonymization and de-identification policy; privacy data anonymization and de-identification policy procedures; other relevant documents or records.	

DM-02: DATA RETENTION AND DISPOSAL

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
PII: The organization: a. Retains each collection of PII for the time period specified by the State Records Retention Schedule in consultation with the Records Management Officer to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with MP-06 and approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses FIPS-validated techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Both the Privacy Act and the Federal Records Act require records to be maintained and disposed of in accordance with a published Records Schedule. Disposal and destruction of PII must be done securely so that it may not be reconstructed. NARA provides retention schedules that govern the disposition of federal records. Program officials and Information Owner(s)/Custodian(s) coordinate with records officers, Cyber Risk Advisor, and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security Numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche may not permit the removal of individual records without the destruction of the entire database contained on such media.	
REFERENCES	**RELATED CONTROLS**

Federal: CFR: 45 C.F.R. §164.310(d)(2)(i), 45 C.F.R. §164.316(b)(2)(i), 45 C.F.R. §164.530(j)(2); Code: 44 U.S.C. Chapter 29, Chapter 31, Chapter 33, 5 U.S.C. §552a(e)(4)(E); E-Gov: §208(e); NIST SP: 800-88; OMB Memo: M-07-16; OMB Circular A-130:; Privacy Act: §552a(c)(2), §552a(e)(1)	AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-01

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization retains each collection of PII for minimum allowable necessary to fulfill the purpose(s) identified in the notice or as required by law;
(ii) The organization disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
(iii) The organization uses legally compliant techniques or methods (as defined in NIST SP 800-88 as amended) to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Determine if:
(i) The system only retains PII pre-determined to be necessary in the authorized data store(s);
(ii) The system has a mechanism for tracking the retention periods associated with the PII it contains;
(iii) The system only retains PII for the length of time specified in the applicable Records Control Schedules;
(iv) Backup schedules are designed in accordance with the applicable Records Control Schedules, for systems that handle the backup process;
(v) All instances and formats of each PII data element are locatable and must be deleted when any one instance of that PII is deleted;
(vi) The system supports clean-up of temporary storage it generates in a manner consistent with the retention needs of the system; and
(vii) The system propagates all authorized deletions of PII to target systems in accordance with requirements, for systems that share PII with other systems.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization PII retention policy; PII retention procedures; organization PII disposal policy; PII disposal procedures; other relevant documents or records.
Examine: The system architecture and identify the PII stored by the system.
Examine: Test records processed by the system.
Examine: Interfaces to the data stores to verify that PII is being saved in the intended data stores.
Test: Attempt to use the system to save PII to an unauthorized data store. Comment: Consider the impact of cloud computing, shared disk arrays, and other technologies in identifying the risk of saving information to an incorrect location.
Examine: The data model and data store architecture for retention tracking. Comment: Data tags, date stamps, metadata, and other mechanisms may be used to support this requirement.
Examine: Test data in the system for association with relevant retention periods.
Test: Instantiate test data with a designated retention period and observe what happens when the retention period expires. Comment: Unless there is a business need to retain PII for historical purposes, it should be deleted when no longer needed.
Examine: The backup scripts and procedures to ensure PII is backed up in a manner that is consistent with the retention periods defined in the Records Control Schedules.
Comment: Records Control Schedules may vary from system to system. The test assumes that the cognizant authority has approved the Records Control Schedules and that these are consistent with the retention periods documented in the SORN(s) that cover this system. The schedule for rotation and overwriting backup media should be considered to further ensure retention periods are not exceeded.
Examine: Deletion routine for search and delete functionality.
Test: Load test input data so as to produce multiple instances of processed PII. Initiate processing and deletion, then manually query the database for the presence of each instance of PII.
Examine: The designated locations for temp files created by the system's normal processes. Review the contents of any persistent temp files following a transaction or process involving PII.
Test: Dump the memory contents created by the system's normal processes and review for presence of PII following a transaction or process involving PII. Comment: Heavily system dependent, impacted by operating system, development platform, and specific application code.
Test: Load input test PII into the system. Delete the test PII and confirm that a deletion message was transmitted to applicable target systems. Comment: Deleting downstream PII is not always an appropriate business decision. This test will depend on the documented purposes and requirements of the target systems.

DM-02(01): SYSTEM CONFIGURATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under a State-approved Records Retention Schedule.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
HIPAA requires the organization to follow specific procedures for de-identification and to implement policies and procedures to address the final disposition of PHI and/or the hardware or electronic media on which it is stored.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.310(d)(2)(i), 45 C.F.R. §164.514	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Information system configuration documentation; information system PII audit records; other relevant documents or records. Confirm that information system PII audit records and other relevant documents or records show that information system configures to record the date PII is collected, created or updated and when PII is to be deleted or archived under the approved record retention schedule.	

DM-03: MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Develops policies and procedures that minimize the use of PII for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
When developing and testing information systems, PII is at a heightened risk for accidental loss, theft, or compromise. Therefore the organization needs to take measures to reduce that risk. Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. The use of PII in testing, research, and training increases risk of unauthorized disclosure or misuse of the information. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. Organizations consult with the Senior Official for Privacy (SOP) and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected. When PII is of a sufficiently sensitive nature, to the greatest extent possible, PII should not be used when testing or developing an information system. **CMS-MARS-E:** Specific to SBMs: 45 CFR §155.1210 Maintenance of Records states the SBMs must maintain and ensure contractors, subcontractors, and agents maintain certain documents and records for 10 years. These documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices, must be sufficient to: accommodate periodic auditing of financial records, and enable HHS or its designee(s) to inspect facilities, or otherwise evaluate the SBM's compliance with federal standards. The requirement further states that the records include, at a minimum, the following: SBMs are required to maintain a record and data retention schedule. Other federal or state laws or regulations may require, or allow, data within this record set to be destroyed earlier than the retention period required by §155.1210. However, SBMs must adhere to the record retention timeframes as described in the Marketplace regulations.	

Specific to Medicaid/CHIP AEs: Medicaid and CHIP performing ACA Administering Entity functions must comply with the records retention requirements that apply to SBMs as well as Records Retention requirement

HIPAA:
HIPAA has specific requirements for the use of PHI in training or research. Under the Health care operations definition, covered entities may use PHI for conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities. For additional information on the use of PHI in research, see 45 C.F.R. §164.512(i).

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization develops policies and procedures that minimize the use of PII for testing, training, and research; and
(ii) The organization implements controls to protect PII used for testing, training, and research.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization policies concerning the use of PII used for testing, training, and research; procedures concerning the use of PII used for testing, training, and research; controls used to protect PII used for testing, training, and research; other relevant documents or records. Confirm that organization does not use PII for testing or training. If they do, confirm that they have documentation describing how the data is protected. Verify the data is protected as described.

DM-03(01): RISK MINIMIZATION TECHNIQUES

Priority: P1

Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E

CONTROL REQUIREMENTS

The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

CONTROL IMPLEMENTATION STANDARDS

Anonymizing PII is one technique to reduce risk and decreases the potential impact if the PII is compromised. Organizations can minimize risk to privacy of PII by using techniques such as de-identification.

When PII is of a sufficiently sensitive nature, to the maximum extent possible, PII should be anonymized in accordance with NIST SP 800-122 prior to its use in development or testing.

SUPPLEMENTAL GUIDANCE

Under HIPAA, there are three requirements that minimize the risk to privacy of using PHI for research, testing or training. The first is the de-identification of information that results in that information no longer being classified as PHI. There are only two methods for de-identification permitted by HIPAA. For specific details on those two methods see 45 C.F.R. §164.514(a). The second requirement is commonly referred to as the “Minimum Necessary Rule” which limits the amount of PHI used or disclosed to that which is reasonably necessary to accomplish the purpose for which the request for information is made. See 45 §C.F.R. §164.514(d). The third requirement allows covered entities to use or disclose a limited data set, which excludes certain direct identifiers. Unlike de-identified data, a limited data set is PHI and any use or disclosure must meet the requirements of HIPAA. See 45 C.F.R. §164.514(e).

REFERENCES	RELATED CONTROLS

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if the organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization policies to minimize the risk of using PII for testing, training, and research; procedures to minimize the risk of using PII for testing, training, and research; techniques used to minimize the risk of using PII for testing, training, and research; other relevant documents or records.

DM-CMS-01: DATA MINIMIZATION AND RETENTION CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. Data Minimization and Retention policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Data Minimization and Retention policy and associated Data Minimization and Retention controls; and b. Reviews and updates (as necessary) the current: 1. Data Minimization and Retention policy at least every two (2) years; and 2. Data Minimization and Retention procedures at least every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the DM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 44 U.S.C. Chapter 29, Chapter 31, Chapter 33; E-Gov: §208(b), §208(e); NIST SP: 800-88, 800-122; OMB Memo: M-03-22, M-07-16; OMB Circular A-130:; Privacy Act: §552a(c)(2), §552a(e), §552a(e)(1)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Data minimization and retention policy and procedures and other relevant documents. Interview: Organizational personnel with data minimization and retention responsibilities to ensure responsibilities are acknowledged.	

(IP) INDIVIDUAL PARTICIPATION AND REDRESS

This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.

IP-01: CONSENT

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;	

b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;
c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and
d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Individual participation and agreement to provide information is fundamental to an individual making an informed decision regarding the collection, use, and safeguarding of their PII. Consent is fundamental to the participation of individuals in the decision-making process regarding the collection and use of their PII and the use of technologies that may increase risk to personal privacy. To obtain consent, organizations provide individuals appropriate notice of the purposes of the PII collection or technology use and a means for individuals to consent to the activity. Organizations tailor the public notice and consent mechanisms to meet operational needs. Organizations achieve awareness and consent, for example, through updated public notices. Organizations may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. For example, opt-in consent may require an individual to click a radio button on a website, or sign a document providing consent. In contrast, opt-out requires individuals to take action to prevent the new or continued collection or use of such PII. For example, the Federal Trade Commission's Do-Not-Call Registry allows individuals to opt-out of receiving unsolicited telemarketing calls by requesting to be added to a list. Implied consent is the least preferred method and should be used in limited circumstances. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII.

Organizational consent mechanisms include a discussion of the consequences to individuals of failure to provide PII. Consequences can vary from organization to organization. Whenever feasible, opt-in is the preferred method to obtain consent.

HIPAA:
Consent is a term under HIPAA with specific meaning not equivalent to a HIPAA authorization. For example, see: Uses and disclosures to carry out treatment, payment, or health care operations (45 C.F.R. §164.506); Uses and Disclosures for Which an Authorization is Required (45 C.F.R. §164.508); Uses and Disclosures Requiring an Opportunity to Agree/Object (45 C.F.R. §164.510); Right to Request Privacy Protection for Protected Health Information (45 C.F.R. §164.522).

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.506(b), 45 C.F.R. §164.508, 45 C.F.R. §164.510, 45 C.F.R. §164.522; Code: 5 U.S.C. §552a(e)(3)-(4); E-Gov: §208(c); OMB Memo: M-03-22, M-10-22; Privacy Act: §552a(b), §552a(e)(3)	AP-1, TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection;
(ii) The organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use,
dissemination, and retention of PII;
(iii) The organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII;
(iv) The organization ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time
the organization collected the PII; and
(v) The user is given the opportunity to provide consent if the system collects PII from that user.
Determine if:

(i) The system input interfaces denote specific PII elements that users are required to provide and clearly note that providing all other PII is optional, for systems that collect PII directly from individuals; and (ii) The system supports a method of tracking consent when appropriate, for systems that collect PII from sources other than the individual.
ASSESSMENT METHODS AND OBJECTS
Examine: Organization policy that authorizes the collection, use, maintaining, and sharing of PII prior to its collection; procedures to authorize the collection, use, maintaining, and sharing of PII prior to its collection; other relevant documents or records. Examine: Input screens to verify that user view contains instructions noting the distinction between required and optional PII. Examine: Input screens to verify that user view clearly marks required data elements. Examine: Test record for the pre-determined method of tracking/flagging consent. Comment: There are multiple scenarios where this requirement may apply, such as when new PII is created or PII is disclosed in new ways, when legal decisions are made, or when decisions regarding benefits are made. This test will require close coordination with the Information Owner(s)/Custodian(s) to determine specifics. “Consent” refers to providing individuals the opportunity to give permission regarding how the agency collects, uses, and discloses their PII, including the decision whether to provide PII when practicable. Where consent is relevant, flags or metadata can be used in the record to denote the types of consent allowed and the level of consent provided by the individual. Test: Create test record with the consent flag enabled and one with the consent flag disabled. Attempt to execute an action that requires use of the consent flag.

IP-01(01): MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization implements mechanisms to support itemized or tiered consent for specific uses of data.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual’s protected health information (PHI). Organizations can provide, for example, individuals’ itemized choices as to whether they wish to be contacted for any of a variety of purposes. In this situation, organizations construct consent mechanisms to ensure that organizational operations comply with individual choices. **HIPAA:** Individual consent or authorization is required under the HIPAA Privacy Rule for uses and/or disclosures of an individual’s PHI.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.506(b), 45 C.F.R. §164.508	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the system employs a mechanism that supports user-provided consent regarding how their personally identifiable information (PII) is used within the system.	
ASSESSMENT METHODS AND OBJECTS	
PII: Examine: Determine that the system employs a mechanism which support user-provided consent regarding how their PII is used within the system.	

IP-02: INDIVIDUAL ACCESS

Priority: P1	
Baseline(s):	Overlay(s):CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Provides individuals the ability to have access to their PII maintained in its system(s) of records;	

b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
c. Publishes access procedures in SORNs; and
d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

CONTROL IMPLEMENTATION STANDARDS

Std.1 - Implement policies and procedures to comply with the regulatory requirements governing an individual's right to access copies of their PHI, including electronic copies.

SUPPLEMENTAL GUIDANCE

The Individual Participation Fair Information Practice Principles (FIPP) requires organizations to provide mechanisms for individuals to gain access to their PII when appropriate. The Privacy Act of 1974, as amended, requires organizations to provide mechanisms for individuals to gain access to their PII when that PII meets the definition of a "record." Access is also an important aspect of supporting correction of PII and redress against alleged violations and misuse of their PII. In addition to access requirements under the Privacy Act of 1974, as amended, HIPAA has statutory requirements to provide access to PHI. Access affords individuals the ability to review PII about them held within organizational systems of records. Access includes timely, simplified, and inexpensive access to data.

Organizational processes for allowing access to records may differ based on resources, legal requirements, or other factors. The Senior Official for Privacy (SOP) working with the Privacy Act Officer is responsible for the content of Privacy Act regulations and record request processing, in consultation with legal counsel. Access to certain types of records may not be appropriate, however, and heads of agencies may promulgate rules exempting particular systems from the access provision of the Privacy Act. In addition, individuals are not entitled to access to information compiled in reasonable anticipation of a civil action or proceeding.
Organizations must provide for public access to records, including PII not included in a Privacy Act System of Records, where required or appropriate. While the language of this control is specific to the Privacy Act's requirements for access, FIPPs encourage organizations to use available authorities to provide access when the Privacy Act does not apply. For example, some organizations use the Freedom of Information Act as another tool to provide access to PII for an affected individual.

CMS-MARS-E:
A state agency (Medicaid/CHIP) or State-based Marketplace that collects personally identifiable information must adhere to state laws that may require granting access to the records or information maintained in the state agency's records similar to the Privacy Act's requirements and the DHHS Privacy Act regulations.

REFERENCES	RELATED CONTROLS
	AR-8, IP-03, TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization provides individuals the ability to have access to their PII maintained in its system(s) of records;
(ii) The organization publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;
(iii) The organization publishes access procedures in SORNs;
(iv) The organization adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests; and
(v) The organization has posted notice to the public for systems that use and collect PII, stating that individuals are allowed to access and view their own PII that the system is storing.
Determine if:
(i) The system provides immediate notification of the right to and the circumstances under which the individual may access their PII, for systems where individuals directly enter
their PII;
(ii) The system enables the individual to review their PII before submitting it for processing, for systems where individuals directly enter their PII; and (iii) The individual has the ability to verify their PII, where authorized, prior to any adverse action being taken on the basis of that PII, for systems that collect PII from a third party.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization policy providing individuals access to their PII maintained in system(s) of records; procedures providing individuals access to their PII maintained in system(s) of record; rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; access procedures in system of records notices (SORN); other relevant documents or records.

Examine: If the system uses and collects PII, confirm they have publically available documents that allows individuals to access and view their own PII that the system is storing. Test: Submit test PII to the system and observe any notice provided. Test: Submit test PII to the system. Comment: This requirement applies to all systems that collect PII directly from the individual. Test: Submit test PII to the system as a third party. Comment: Applies to all systems that collect PII from third parties. Test: Submit test PII to the system as a third party which produces actionable output. Comment: Applies only to systems that produce actionable output.

IP-03: REDRESS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Redress supports data integrity requirements for PII by providing a process for individuals to request correction of, or amendment to, their PII maintained by an organization. Redress supports the ability of individuals to ensure the accuracy of PII held by organizations. Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations use discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought, and the impact of the changes. Individuals may appeal an adverse decision and have incorrect information amended, where appropriate. To provide effective redress, organizations: (i) provide effective notice of the existence of a PII collection; (ii) provide plain language explanations of the processes and mechanisms for requesting access to records; (iii) establish criteria for submitting requests for correction or amendment; (iv) implement resources to analyze and adjudicate requests; (v) implement means of correcting or amending data collections; and (vi) review any decisions that may have been the result of inaccurate information. Organizational redress processes provide responses to individuals of decisions to deny requests for correction or amendment, including the reasons for those decisions, a means to record individual objections to the organizational decisions, and a means of requesting organizational reviews of the initial determinations. Where PII is corrected or amended, organizations take steps to ensure that all authorized recipients of that PII are informed of the corrected or amended information. In instances where redress involves information obtained from other organizations, redress processes include coordination with organizations that originally collected the information.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.526; Code: 5 U.S.C. §552a(c)(4), (d), and (h); OMB Circular A-130; Privacy Act: §552a(c)(4), §552a(d)	IP-02, TR-01, TR-02, UL-02, DI-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization provides a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; (ii) The organization establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended; and (iii) The redress policy and procedures allow an individual to make corrections to any information about that individual. Determine if: (i) The system notifies the individual either directly or indirectly of adverse output based on PII submitted to the system and notify the individual of the mechanisms for redress;	

(ii) The system notifies the third parties of the mechanisms and circumstances governing the update/ correction of the submitted PII, for systems that receive PII from third parties; (iii) The system enables them to update/correct submitted PII, for systems that receive PII from third parties; (iv) The system enables them to update/correct the submitted PII, for systems that receive PII from source systems; (v) The system provides immediate notification of the right to and the circumstances under which the individual may update/correct their PII, for systems into which individuals directly enter their PII; (vi) The system maintains a flag indicating that the PII is in dispute, when the individual disputes the accuracy of PII or any output based on the disputed PII; and (vii) the system propagates all authorized updates/corrections of PII to target systems.
ASSESSMENT METHODS AND OBJECTS
Examine: Redress process policy and procedure. Test: Submit test PII that results in adverse output. Comment: This requirement applies to systems that may produce adverse actionable output based on PII. Test: Submit test PII as a third party to the system and observe any notice provided. Comment: This requirement applies to all systems that collect, process, or transmit PII. Test: Submit test PII to the system as a third party, then attempt to update the test PII originally submitted. Comment: This requirement applies to all systems that collect, process, or transmit PII. Test: Submit test PII to the system from a source system, then attempt to update the test PII originally submitted. Comment: This requirement applies to all systems that collect, process, or transmit PII. Test: Enter test PII into the system and observe any notice provided. Comment: This requirement applies to all systems that collect, process, or transmit PII. Test: Submit test PII to the system. Subsequently submit a dispute of the same PII. Comment: This requirement applies to systems that may produce adverse actionable output based on PII. Test: Submit updated test PII to the system and verify that the update is transmitted to target systems.

IP-04: COMPLAINT MANAGEMENT

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Establishing a complaint management process ensures complaints are addressed in a timely manner and provides an avenue for individuals to participate in government activities that may impact privacy. Information received from complaints provides external input regarding organizational privacy and security practices which may improve processes and systems involved in collection, use, and maintenance of personally identifiable information (PII). Complaints, concerns, and questions from individuals can serve as a valuable source of external input that ultimately improves operational models, uses of technology, data collection practices, and privacy and security safeguards. Organizations provide complaint mechanisms that are readily accessible by the public, include all information necessary for successfully filing complaints (including contact information for the Senior Official for Privacy (SOP) or other official designated to receive complaints), and are easy to use. Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.530 (d); OMB Memo: M-07-16, M-08-09; OMB Circular A-130: 7.g.	AR-6, IP-03
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if there are adequate procedures for handling privacy related inquiries and complaints.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Procedural documents for handling privacy related inquiries and complaints. Interview: The ISSO and/or Data Guardian and request a list of personnel who is responsible for managing the complaints.	

Examine: Sample inquiries and complaints.

IP-04(01): RESPONSE TIMES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization: a. Acknowledges complaints, concerns, or questions from individuals within ten (10) working days; b. Completes review of requests within thirty (30) working days of receipt, unless unusual or exceptional circumstances preclude completing action by that time; and c. Responds to any appeal as soon as possible, but no later than thirty (30) working days after receipt of the appeal unless the appeal authority can show good cause to extend the response period.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Timely communication and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under HIPAA. Timely communication and resolution of complaints from individuals demonstrates responsiveness by the organization and reduces the organization's risk of reputational damage and potential lawsuits under the Privacy Act. Organizations should establish a complaint management process that ensures complaints are resolved within a reasonable amount of time.	
REFERENCES	**RELATED CONTROLS**
Federal: 45 CFR § 164.524	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization responds to complaints, concerns, or questions from individuals within the CMS-defined time period.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Process for responding to complaints, concerns, or questions from individuals; other relevant documents or records.	

IP-CMS-01: INDIVIDUAL PARTICIPATION AND REDRESS CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. Individual Participation and Redress policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Individual Participation and Redress policy and associated Individual Participation and Redress controls; and b. Reviews and updates (as necessary) the current: 1. Individual Participation and Redress policy at least every two (2) years; and 2. Individual Participation and Redress procedures at least every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular	

information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
E-Gov: §208(c); OMB Memo: M-03-22, M-07-16, M-08-09, M-10-22; OMB Circular A-130:; Privacy Act: §552a(b), §552a(c)(3), §552a(c)(4), §552a(d), §552a(d)(5), §552a(e)(3), §552a(e)(4), §552a(j), §552a(k), §552a(t)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Individual participation and redress policy and procedures, and other relevant documents. Interview: Organizational personnel with individual participation and redress responsibilities to ensure responsibilities are acknowledged.	

(SE) SECURITY

This family supplements the security controls in Appendix F to ensure administrative, technical, and physical measures are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with Office of Management and Budget (OMB) policies and guidance. The controls in this family are implemented in coordination with information security personnel using the existing NIST Risk Management Framework.

SE-01: INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Establishes, maintains, and updates, no less often than once every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII; and b. Provides each update of the PII inventory to the HHS Senior Official for Privacy (SOP) and the HHS CISO no less often than once every three hundred sixty-five 365 days to support the establishment of information security requirements for all new or modified information systems containing PII.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
The PII inventory identifies the organization's information assets and identifies those assets collecting, using, maintaining, or sharing PII. The PII inventory identifies those assets most likely to impact privacy; provides a starting point for organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII; and to mitigate risks of PII exposure. The PII inventory enables organizations to identify systems and programs that contain PII so that they can then identify and address privacy risks. The PII inventory identifies: (i) the name and acronym for each program and system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII as collected, used, maintained, or shared by that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations gather information on the location of PII as they are developing and updating systems and programs. In addition, they cross reference information in privacy impact assessments (PIA) and system of records notices (SORN) to ensure that PIAs and SORNs are consistent with the PII inventory. Organizations may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of	

substantial harm, embarrassment, inconvenience, or unfairness to affected individuals, as well as the financial or reputational risks to organizations, if PII is exposed. Organizations take due care in creating and updating the inventories by identifying linkable data that could create PII.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.530(c); 45 C.F.R. §164.310(d); Code: 5 U.S.C. §552a(e)(10); Pub. L. No. 107-347, §208(b)(2); E-Gov: §208(b)(2); FIPS Pub: 199; NIST SP: 800-37, 800-122; OMB Memo: M-03-22, M-07-16 Att. 1, B.1.a, M-16-04; OMB Circular A-130: Appendix I; Privacy Act: §552a(e)(10)	AR-1, AR-4, AR-5, AT-1, CM-8, DM-1, PM-5

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization establishes, maintains, and updates, no less often than once every three hundred sixty-five (365) days, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII;
(ii) The organization provides each update of the PII inventory to the SOP and the CISO to support the establishment of information security requirements for all new or modified information systems containing PII; and
(iii) The inventory list of all systems that are collecting and maintaining PII are accurate and complete.

ASSESSMENT METHODS AND OBJECTS

Examine: Request and review the inventory list of all systems that are collecting and maintaining PII.

SE-02: PRIVACY INCIDENT RESPONSE

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA

CONTROL REQUIREMENTS

The organization:
a. Develops and implements a Privacy Incident and Breach Response Plan; and
b. Provides an organized and effective response to privacy incidents and breaches in accordance with HHS and CMS Privacy Incident (and Breach) Response Plans.

CMS-MARS-E:
c. The organization follows current CMS Incident Reporting requirements for reporting incidents to oversight organizations as defined in the incident handling documents available at:
https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

CONTROL IMPLEMENTATION STANDARDS

SUPPLEMENTAL GUIDANCE

Developing and implementing a risk-based analysis for privacy breaches using a “Best Judgment Standard” as described in this control’s supplemental guidance ensures consistency in, and avoids over-reporting of, privacy breach notifications.

The organizational Privacy Incident and Breach Response Plan may be integrated with the organizational Incident Response Plan. The organization privacy incident and breach response capability must be able to demonstrate knowledge of the privacy incident and breach response processes and procedures and evidence showing the plan is followed routinely while responding to privacy incidents and breaches.

In contrast to the Incident Response (IR) family in NIST 800-53 Appendix F, which concerns a broader range of incidents affecting information security, this control uses the term Privacy Incident to describe only those incidents that relate to personally identifiable information (PII). The organization Privacy Incident Response Plan is developed under the leadership of the Senior Official for Privacy (SOP). The plan includes:
(i) The establishment of a cross-functional Privacy Incident Response Team that reviews, approves, and participates in the execution of the Privacy Incident Response Plan;
(ii) A process to determine whether notice to oversight organizations or affected individuals is appropriate and to provide that notice accordingly;
(iii) A privacy risk assessment process to determine the extent of harm, embarrassment, inconvenience, or unfairness to affected individuals and, where appropriate, to take steps to mitigate any such risks;
(iv) Internal procedures to ensure prompt reporting by employees and contractors of any privacy incident to the SOP and other designated officials consistent with organizational incident management structures; and

(v) Internal procedures for reporting noncompliance with organizational privacy policy by employees or contractors to appropriate management or oversight officials. Some organizations may be required by law or policy to provide notice to oversight organizations in the event of a breach.
Organizations may also choose to integrate Privacy Incident Response Plans with Security Incident Response Plans or keep the plans separate.

The Best Judgment Standard, explained in OMB M-07-16, Footnote 6, imposes a requirement for organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. The Best Judgment Standard gives organizations responsibility for their own data in two important ways. First, the organization must determine the sensitivity of its PII, based on the information and the context in which the information appears. Second, the organization must determine whether a privacy breach should be reported, based on the resultant privacy risk to the organization and to affected individuals. The Best Judgment Standard effectively imposes a requirement on organizations to develop and implement a risk-based analysis for privacy breaches to determine whether the breach needs to be reported. In the context of breach reporting, the purpose of the Best Judgment Standard is to limit reporting to those privacy breaches which meet the organization's risk threshold.

Conversely, under the Best Judgment Standard, organizations are not required to report privacy breaches that do not meet their risk threshold. The policy provides an example of implementing the Best Judgment Standard as discarding a document with the author's name on the front and no other PII into an office trashcan, positing that this probably would fall below and organization's risk threshold and would not need to be reported.
OMB M-07-16 does not provide bright line rules to define what is considered "sensitive PII" using the common dictionary definition approach to the language in the memorandum–and under what circumstances a privacy breach should be reported, both because it would be a futile effort to attempt to delineate or predict the myriad potential contexts and situations, and agencies are in the best position to know and understand the relevant circumstances of their PII to determine which PII is sensitive and which breaches create risk.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. Part 164 Subpart D; 45 C.F.R. §164.308(a)(6); NIST SP: 800-37; OMB Memo: M-06-19, M-07-16; Privacy Act: §552a(e), §552a(i)(1), §552a(m)	AR-1, AR-4, AR-5, AR-6, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, RA-1

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization develops and implements a Privacy Incident and Breach Response Plan; and
(ii) The organization provides an organized and effective response to privacy incidents and breaches in accordance with HHS and CMS Privacy Incident (and Breach) Response Plans.
Determine if there is a privacy incident response plan.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization Privacy Incident Response Plan; privacy incident response procedures; other relevant documents or records.
Interview: Organizational personnel with privacy incident and breach response planning responsibilities.
Test: Organizational privacy incident and breach response plan and related organizational processes.
Examine: Review the Privacy Incident Response Plan or verify a privacy section is present with the ISRA and accurately reflect CMSR v. 2.0 guidelines.

SE-CMS-01: SECURITY CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS

CONTROL REQUIREMENTS

The organization:
a. Develops, documents, and disseminates to applicable personnel:
1. Security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the Security policy and associated Security controls; and
b. Reviews and updates (as necessary) the current:
1. Security policy at least every two (2) years; and
2. Security procedures at least every two (2) years.

CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as "Limited Applicability - System does not process PII nor PHI."	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: E-Gov: §208(b)(2); FIPS Pub: 199; NIST SP: 800-37, 800-122; OMB Memo: M-06-19, M-07-16, M-03-22, M-16-04; OMB Circular A-130: Appendix I; Privacy Act: §552a(e), §552a(e)(10), §552a(i)(1), §552a(m)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Privacy's security policy and procedures, and other relevant documents. Interview: Organizational personnel with privacy's security responsibilities to ensure responsibilities are acknowledged.	

(TR) TRANSPARENCY

This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities.

TR-01: PRIVACY NOTICE

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Provides effective notice to the public and to individuals regarding: 1. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII; 2. Authority for collecting PII; 3. The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and 4. The ability to access and have PII amended or corrected if necessary. b. Describes: 1. The PII the organization collects and the purpose(s) for which it collects that information; 2. How the organization uses PII internally; 3. Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; 4. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; 5. How individuals may obtain access to PII; and 6. How the PII will be protected. c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	

Providing the appropriate notification of privacy practices to the individual enables the individual to make an informed decision when they provide their consent.

Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including system of records notices (SORN), privacy impact assessments (PIA), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The Senior Official for Privacy (SOP) is responsible for the content of the organization's public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization's compliance with the public notice provisions of the Privacy Act, the E-Government Act's PIA requirement, with OMB guidance related to federal agency privacy notices. Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SOP and Chief Counsel.

The Privacy Notice described by OMB M-99-18, Privacy Policies on Federal Web Sites, frequently referred to on organization websites as a "Privacy Policy" or "Privacy and Security Notice," is intended as a broad notice of website privacy policies and general website use and does not meet the requirement for specific notice when collecting PII. When PII is maintained (including collected) in a system of records that is covered by the Privacy Act, the organization must provide a "Privacy Act Statement" (PAS) to the individual at the time of collection that meets the requirements of the Privacy Act of 1974, 5 U.S.C. §552a(e)(3), unless the organization has published a rule exempting that system of records from the (e)(3) notice provision in accordance with subsection (j) of the Privacy Act. If the PII is not maintained in a system of records under the Privacy Act, a privacy notice should be provided which describes the privacy practices associated with that PII, including, but not limited to, the way the PII is protected, how it is used, and whether it is shared. This type of privacy notice must not be labeled as a "Privacy Act Statement." For example, several organizations refer to this notice type as a "Privacy Advisory."

HIPAA:
The HIPAA Privacy Rule also requires a privacy notice referred to as a "Notice of Privacy Practices." For specific rules on this notice please refer to 45 C.F.R. §164.520.

REFERENCES	RELATED CONTROLS
	AP-1, AP-2, AR-1, AR-2, IP-01, IP-02, IP-03, UL-01, UL-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization provides effective notice to the public and to individuals regarding their privacy program policies and practices that includes:
- its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;
- Authority for collecting PII;
- The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and
- The ability to access and have PII amended or corrected if necessary.
(ii) The organization describes:
- The PII the organization collects and the purpose(s) for which it collects that information;
- How the organization uses PII internally;
- Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing;
- Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent;
- How individuals may obtain access to PII; and
- How the PII will be protected.
(iii) The organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Determine if privacy notices are accurate and complete for systems that collect PII. Determine if the system provides notice of the privacy practices associated with the system, the PII collected, and a description of how the PII is used and managed, for systems that collect PII directly from individuals.
ASSESSMENT METHODS AND OBJECTS
Examine: Public notice regarding individual privacy and PII; other relevant documents or records. Examine: If the system collects PII, confirm it has a privacy notice that describes: (i) The PII the organization collects and the purpose(s) for which it collects that information; (ii) How the organization uses PII internally; (iii) Whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) How individuals may obtain access to PII; and (vi) How the PII will be protected. Test: Attempt to enter test PII as an individual using the system. Observe any notice provided by the system. Comment: Notice at the point of collecting PII directly from the individual allows for the assumption that the individual is providing consent for the PII collected and the purposes for which it will be used. There are various methods of providing notices through systems, depending on the purposes of the system. For example, notice may be provided through the website privacy policy, as a pop-up box, end-user agreement, or as text located above the input fields for PII.

TR-01(01): REAL-TIME OR LAYERED NOTICE

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	
The organization provides real-time and/or layered notice when it collects PII.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Real-time notice facilitates informed consent and promotes trust from the individual when collecting sensitive PII. Real-time notice used in conjunction with a Privacy Act Statement or Privacy Advisory, based on the sensitivity of the PII provided or collected, ensures the individual provides informed consent. Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization's privacy policy. A second notice provides more detailed/specific information. **HIPAA:** The HIPAA Privacy Rule provides the option of layered notice to allow for simplified up-front notification with greater detail following. The Department of Health and Human Services has provided both guidance and model notices of privacy practices (see http://www.hh.gov/ocr/privacy/hipaa/modelnotices.html for details).	
REFERENCES	**RELATED CONTROLS**
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if a privacy notice is placed at the point of collections for systems that collect PII.	
ASSESSMENT METHODS AND OBJECTS	
Examine: If the system collects PII, verify a privacy notice is placed at the point of collection.	

TR-02: SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	

Non-Federal systems are not required to implement this control. State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement. The organization, through the HHS Privacy Act Officer, OpDiv Privacy Contacts, and the HHS Office of General Counsel: a. Publishes SORNs in the Federal Register, subject to required oversight processes, for systems containing PII; b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.
CONTROL IMPLEMENTATION STANDARDS
SUPPLEMENTAL GUIDANCE
SORNs and Privacy Act Statements, i.e., (e)(3) notices, provide transparency, in advance of collection, use, maintenance, or sharing of PII when in a system that meets the statutory definition of a "system of records" under the Privacy Act. The Privacy Act defines "maintain" as "maintain, collect, use or disseminate." These requirements impact decisions made during planning, design, development, and operation of programs and systems. Organizations issue SORNs to provide the public notice regarding PII collected in a system of records, which the Privacy Act defines as "a group of any records under the control of any agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifier." SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. Privacy Act Statements provide notice of: (i) the authority of organizations to collect PII; (ii) whether providing PII is mandatory or optional; (iii) the principal purpose(s) for which the PII is to be used; (iv) the intended disclosures (routine uses) of the information; and (v) the consequences of not providing all or some portion of the information requested. When information is collected verbally, organizations read a Privacy Act Statement prior to initiating the collection of PII (for example, when conducting telephone interviews or surveys). The Privacy Act and OMB guidance set forth specific requirements regarding when and how notices are provided. In addition to any internal organization review process, the publication of a SORN in the Federal Register requires a mandatory review and comment period of a minimum of 40 days. Regarding TR-02, paragraph a, the publication of a SORN is required only when the PII is maintained in a system that meets the statutory definition of a "system of records" under the Privacy Act. Not all systems containing PII may meet the definition of a "system of records." However, all PII maintained by an organization must be protected irrespective of whether the PII is subject to the Privacy Act. Regarding TR-02, paragraph c, the Privacy Act Statement (PAS), when required, should be provided in the same format as the information is collected. For example, an electronic statement on a website, a written statement on a paper form, and a verbal statement provided for information that is collected verbally.

REFERENCES	RELATED CONTROLS
Federal: Code: 5 U.S.C. §552a(e)(3)-(e)(4); OMB Circular A-130; Privacy Act: §552a(e)(3)	DI-2

ASSESSMENT PROCEDURES
ASSESSMENT OBJECTIVES
Determine if the system has a SORN in the Federal Register.
ASSESSMENT METHODS AND OBJECTS
Examine: Verify the system has a SORN in the Federal Register.

TR-02(01): PUBLIC WEBSITE PUBLICATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E
CONTROL REQUIREMENTS	

Non-Federal systems are not required to implement this control. State-based systems must adhere to state laws that may require publication of a notice similar to the federal SORN and Privacy Act Statement. The organization publishes SORNs on its public website.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - SORNs must be published on the CMS systems of records website at http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/CMS-Systems-of-Records.html	
SUPPLEMENTAL GUIDANCE	
Publishing SORNs on organization websites improves transparency by providing individuals easier access to information about how their PII will be collected, used, maintained, or shared; and centralizing the information regarding to whom an individual should submit a request for access or amendment to their information covered by the SORN. The organization may establish a centralized website for publication of their SORNs.	
REFERENCES	**RELATED CONTROLS**
Federal: 5 U.S.C. §552a(e)(4;); OMB Circular A-130: 7.g. and Appendix I	
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the current SORN is located on the CMS dedicated website.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Verify that the current SORN is located on http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/CMS-Systems-of-Records.html	

TR-03: DISSEMINATION OF PRIVACY PROGRAM INFORMATION

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Official for Privacy (SOP); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.	
CONTROL IMPLEMENTATION STANDARDS	
SUPPLEMENTAL GUIDANCE	
Making information about an organization's privacy program readily available to the public reduces the burden on individuals wanting to better understand an organization's privacy practices; and reduces burden on privacy offices and program officials by providing answers to common privacy questions through an easily accessible forum. Organizations employ different mechanisms for informing the public about their privacy practices including, but not limited to, privacy impact assessments (PIA), system of records notices (SORN), privacy reports, publicly available web pages, email distributions, blogs, and periodic publications (e.g., quarterly newsletters). Organizations also employ publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.	
REFERENCES	**RELATED CONTROLS**
Federal: Code: 5 U.S.C. §552a(e)(4); Pub. L. No. 107-347, §208(b)(1)(B)(iii); E-Gov: §208; OMB Memo: M-03-22, M-10-23 Section 4 Privacy Act: §552a	AR-6
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if information regarding privacy policies are publically available.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Verify information regarding privacy policies are publically available. For example, HHS and CMS maintains program specific privacy policies and documentation at the following websites: HHS Privacy Impact Assessment Page - http://www.hhs.gov/pia/ Information Security and Privacy Library - https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html	

TR-CMS-01: TRANSPARENCY CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. Transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Transparency policy and associated Transparency controls. b. Reviews and updates (as necessary) the current: 1. Transparency policy at least every two (2) years; and 2. Transparency procedures at least every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as “Limited Applicability - System does not process PII nor PHI.”	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the TR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security and privacy program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security and privacy policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.	
REFERENCES	**RELATED CONTROLS**
Federal: E-Gov: §208(b); OMB Memo: M-03-22, M-07-16, M-10-22, M-10-23; OMB Circular A-130:; Privacy Act: §552a, §552a(e)(3), §552a(e)(4)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Transparency policy and procedures, and other relevant documents. Interview: Organizational personnel with transparency responsibilities to ensure responsibilities are acknowledged.	

(UL) USE LIMITATION

This family is intended to assist organizations in complying with the Privacy Act, which prohibits uses of PII that are either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the Controls in this Family will ensure that the scope of PII use is limited accordingly.

UL-01: INTERNAL USER

Priority: P1	
Baseline(s):	Overlay(s): HIPAA, CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - All PII must be used for an official government purpose only. The officers and employees of the organization must have a need for the PII in the performance of their official duties. These requirements apply to all PII regardless of its coverage by the Privacy Act.	
SUPPLEMENTAL GUIDANCE	

Consistent with the Privacy Act, the organization's internal use of PII contained in a system of records notice (SORN) is limited to the purposes identified in one of the 12 exceptions to Section b of the Privacy Act and as described in the SORN. Consistent with the Fair Information Practice Principles (FIPP) and Section 208 of the E-Government Act, the organization's internal use of PII not contained in a SORN should be compatible with the purpose for which it was originally collected and as described in the PIA or other public notice.

Organizations take steps to ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices. These steps include monitoring and auditing organizational use of PII and training organizational personnel on the authorized uses of PII. With guidance from the Senior Official for Privacy (SOP) and where appropriate, legal counsel, organizations document processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities. Where appropriate, organizations obtain consent from individuals for the new use(s) of PII.

The phrase "authorization schema" refers to the logic of how authorization permissions are designed to function within the system (e.g., by group, by role, by transaction type, etc.). An example of an authorization schema where permissions appropriately match functions would be a schema where a group of "reviewers" is separate from a group of "approvers." Individuals assigned to the "reviewer" group could read PII and make recommendations, but not approve actions. Individuals in the "approver" group could read recommendations and approve actions. An authorization schema where all individuals are automatically authorized to approve all actions is an example of a schema where the alignment between permissions and functions may be inappropriate.

REFERENCES	RELATED CONTROLS
Federal: CFR: 45 C.F.R. §164.502; 45 C.F.R. §164.504; 45 C.F.R. §164.506; 45 C.F.R. §164.508; 45 C.F.R. §164.510; 45 C.F.R. §164.512; 45 C.F.R. §164.514 Code: 5 U.S.C. §552a; Pub. L. No. 107-347, §208; OMB Circular A-130: 7.g.; Privacy Act: §552a(b)(1)	AC-2, AC-3, AC-5, AC-6, AC-8, AC-21, AU-2, AU-3, AU-10, AU-14, IA-2, PS-1, PS-2, PS-3, AP-2, AR-2, AR-3, AR-4, AR-5, IP-01, TR-01, TR-02

ASSESSMENT PROCEDURES

ASSESSMENT OBJECTIVES

Determine if:
(i) The organization uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices
Determine if:
(i) The system's use of PII is consistent with the privacy notices related to the system, including SORN, Privacy Impact Assessment, and notices provided at points of collection;
(ii) The system's disclosures of PII are consistent with the privacy notices related to the system, including SORN, Privacy Impact Assessment, and notices provided at points of collection;
(iii) The authorization schema for the system aligns with the business logic within the system;
(iv) The system responds to authorization changes within a defined timeframe;
(v) The system connects to source systems so as to process changes in authorizations based on relevant organizational events (e.g., separations, job changes, etc.); and
(vi) The system requests appropriate credentials at the time of request for initial access so as to sufficiently identify the user/system making the request.

ASSESSMENT METHODS AND OBJECTS

Examine: Organization privacy policy; organization privacy practices; other relevant documents or records.
Examine: Documented system functions with relevant privacy notices.
Examine: Documented system outputs with relevant privacy notices.
Examine: The functions of the system and the authorization schema of the system, and compare them for alignment. Comment: If the authorization schema is not in alignment with business functions it could result in entities having greater access to PII than needed.
Examine: The authorization schema and compare it to the SORN and any applicable Computer Matching Agreements and data sharing memoranda of understanding (MOU)/memoranda of agreement (MOA). Comment: If the authorization schema allows for access or roles that are not included as part of relevant privacy documents, the system will be in violation of the Privacy Act of 1974.
Examine: A sample of the existing or proposed users/systems and compare their business responsibilities to their permissions within the system. Comment: If the authorization schema is too broad, it will result in entities having greater access to PII than needed; if the schema is too narrow, it will result in overly burdensome administration of the system authorizations.
Test: Remove a user/system's authorization to access the system.

Test: Remove a user/system's authorization permission. Test: Reduce the authorization status of a user/system. Examine: The system design to verify that the system connects to all of the appropriate source systems for changes in user/system status. Test: Make a change to a user/system's status in the source system such that access to the system being tested would be removed or reduced (e.g., a separation). Test: Make a change to a user/system's status in the source system such that a specific permission authority would be removed (e.g., a department change). Comment: The number of test cases may vary based on: (1) The PII and processing capabilities of the system; (2) The technology platform of the system; and (3) Connections to any centralized authorization facilities. Test: Attempt to gain access to the system without entering appropriate credentials. Test: Attempt to gain access to the system with valid credentials. Test: Attempt to gain access to the system as multiple users/systems.

UL-02: INFORMATION SHARING WITH THIRD PARTIES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS, CMS-MARS-E, VA
CONTROL REQUIREMENTS	
The organization: a. Shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes; b. Where appropriate, enters into MOUs, MOAs, Letters of Intent, CMAs, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - Consistent with the Purpose Specification and Use Limitation Fair Information Practice Principles (FIPP), sharing of PII must be compatible with the purpose for which it was collected. Consistent with the Transparency FIPP, any subsequent sharing that is not compatible may not be done until additional notice is provided to the individual, their consent is obtained, and relevant documents are updated or published; e.g., when applicable and appropriate publish an updated system of records notice (SORN) to cover the additional incompatible sharing and obtain consent from the affected individuals.	
SUPPLEMENTAL GUIDANCE	
Sharing PII with third parties introduces new risks to the individual which, as applicable, requires organizations to establish formal agreements with the third party and ensure the sharing is compatible with the purposes described in notice to, and consent from, the individual. Consideration of privacy risks for sharing PII apply regardless of the method used or whether the information remains stored in the system of records. Data removed from an information system covered by a system of records notice (e.g., a Human Resources [HR] database) and shared in another format (e.g., an Excel spreadsheet) must still meet purpose and use requirements of the associated notice. PII not in a system of records that is shared with a third party still must meet the Purpose Specification and, relatedly, Use Limitation FIPPs. For example, data extracts of PII shared via an Excel spreadsheet or database archive. A third party is an individual or organization besides CMS and the individual about whom CMS collects and uses information. The organization SOP and, where appropriate, legal counsel review and approve any proposed external sharing of PII, including with other public, international, or private sector entities, for consistency with uses described in the existing organizational public notice(s). When a proposed new instance of external sharing of PII is not currently authorized by the Privacy Act and/or specified in a notice, organizations evaluate whether the proposed external sharing is compatible with the purpose(s) specified in the notice. If the proposed sharing is compatible, organizations review, update, and republish their privacy impact assessment (PIA), SORN, website privacy policies, and other public notices, if any, to include specific descriptions of the new uses(s) and obtain consent where appropriate and feasible. Information-sharing agreements also include security protections consistent with the sensitivity of the information being shared.	

HIPAA: Under the HIPAA, a covered entity may not use, disclose or request a medical record, except when the medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. The disclosure and sharing of PHI is governed by the HIPAA regulations. For details consult the HIPAA Privacy and Security rules at: http://www.hhs.gov/ocr/privacy/index.html.	
REFERENCES	**RELATED CONTROLS**
Federal: CFR: 45 C.F.R. §164.502(e)(1), 45 C.F.R. §164.514(e)(1); Code: 5 U.S.C. §552a; Guide: Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment; Privacy Act: §552a(a)(7), §552a(b), §552a(c), §552a(e)(3)(C), §552a(o)	AP-2, AR-3, AR-4, AR-5, AR-8, DI-1, DI-2, IP-01, TR-01
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if: (i) The organization shares PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes; (ii) The organization where appropriate, enters into MOUs, MOAs, Letters of Intent, CMAs, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; (iii) The organization monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and (iv) The organization evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	
ASSESSMENT METHODS AND OBJECTS	
Examine: Organization privacy policy; organization privacy practices; MOUs, MOAs, Letters of Intent, CMAs, or similar agreements with third parties; system configuration; audit records; training records; and other relevant documents or records.	

UL-CMS-01: USE LIMITATION CONTROL FAMILY POLICY AND PROCEDURES

Priority: P1	
Baseline(s):	Overlay(s): CMS-ARS
CONTROL REQUIREMENTS	
The organization: a. Develops, documents, and disseminates to applicable personnel: 1. Use Limitation policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the Use Limitation policy and associated Use Limitation controls; and b. Reviews and updates (as necessary) the current: 1. Use Limitation policy at least every two (2) years; and 2. Use Limitation procedures at least every two (2) years.	
CONTROL IMPLEMENTATION STANDARDS	
Std.1 - For any system that does not process or store PII and/or PHI, the SSP must document this control family as “Limited Applicability - System does not process PII nor PHI.”	
SUPPLEMENTAL GUIDANCE	
This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the UL family.	
REFERENCES	**RELATED CONTROLS**
Federal: Privacy Act: §552a(a)(7), §552a(b), §552a(b)(1), §552a(c), §552a(e)(3)(C), §552a(o)	AR-1
ASSESSMENT PROCEDURES	
ASSESSMENT OBJECTIVES	
Determine if the organization has implemented all elements of this control as described in the control statements and implementation standard(s).	
ASSESSMENT METHODS AND OBJECTS	
Examine: Use limitation policy and procedures, and other relevant documents. Interview: Organizational personnel with use limitation responsibilities to ensure responsibilities are acknowledged.	

Appendix D: HIPAA Security Rules to IS-Controls Mapping

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
General Rules	General Requirements		164.306(a)	
General Rules	General Requirements		164.306(a)(1)	AU-09(03)
General Rules	General Requirements		164.306(b)	PM-11
Administrative Safeguard	Security management process		164.308(a)(1)(i)	AU-12(03), CA-09(01), PL-02, PL-08, RA-01, RA-05, RA-05(05), SA-03, SA-08, SA-10, SA-11, PM-01, PM-07, PM-09, PM-11
Administrative Safeguard	Security management process		164.308(a)(1)(ii)	PM-09
Administrative Safeguard	Security management process	Risk Analysis	164.308(a)(1)(ii)(A)	CA-09, CM-04, PE-16, PL-08, RA-02, RA-03, SA-05, SA-11, SC-05, PM-08, PM-12, PM-16
Administrative Safeguard	Security management process	Risk Management	164.308(a)(1)(ii)(B)	AC-02(13), CM-04, RA-02, RA-03, SC-05, PM-04, PM-08
Administrative Safeguard	Security management process	Sanction Policy	164.308(a)(1)(ii)(C)	AC-02(13), PS-08
Administrative Safeguard	Security management process	Sanction Policy	164.308(a)(1)(ii)(D)	AC-06(07), AC-06(09), AU-01, AU-02, AU-03, AU-04, AU-06, AU-07, AU-07(01), AU-07(02), AU-09, AU-12, AU-12(03), AU-16(02), CA-07, CM-06, CM-10, CM-11, IR-05, IR-06, IR-08, MA-04, SC-05, SC-07, SC-18, SC-28, SI-04, PM-12, PM-16
Administrative Safeguard	Assigned security responsibility		164.308(a)(2)	AU-12(03), CA-01, CA-05, CA-06, PM-01, PM-02, PM-10, PM-13
Administrative Safeguard	Workforce security		164.308(a)(3)	IA-05
Administrative Safeguard	Workforce security		164.308(a)(3)(i)	AC-01, AC-05, AC-06, AC-06(01), AC-06(05), CM-07, MP-07, PE-18, SC-07, SI-03, PM-01, PM-12, PM-13, PM-16
Administrative Safeguard	Workforce security	Authorization and/or Supervision	164.308(a)(3)(ii)(A)	AC-01, AC-02(09), AC-03, AC-04, AC-06(01), AC-06(05), AC-06(07), AC-21, AU-12, CA-09, CM-10, CM-11, MA-01, MA-02, MA-03, MA-04, MA-05, MP-02, MP-07, PE-01, PE-02, PE-03, PL-08, PS-01, PS-06, PS-07
Administrative Safeguard	Workforce security	Workforce Clearance Procedures	164.308(a)(3)(ii)(B)	AC-02, AC-06(01), AC-06(02), AC-06(05), AC-06(07), PS-01, PS-02, PS-03, PS-03(03), PS-05, PS-06, SA-21
Administrative Safeguard	Workforce security	Termination Procedures	164.308(a)(3)(ii)(C)	AC-02(13), PS-01, PS-04, PS-05

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
Administrative Safeguard	Information access management		164.308(a)(4)	IA-04
Administrative Safeguard	Information access management		164.308(a)(4)(i)	AC-01, AC-02, AC-05, AC-06, AC-06(01), AC-06(07), AC-20, CM-02, CM-07, SC-07, PM-01, PM-08, PM-12, PM-16
Administrative Safeguard	Information access management	Isolating Healthcare Clearinghouse Functions	164.308(a)(4)(ii)(A)	AC-05, AC-06, AC-20
Administrative Safeguard	Information access management	Access Authorizations	164.308(a)(4)(ii)(B)	AC-01, AC-02, AC-02(09), AC-03, AC-04, AC-06(07), AC-21, PS-06, PS-07, SC-07
Administrative Safeguard	Information access management	Access Establishment and Modification	164.308(a)(4)(ii)(C)	AC-01, AC-02, AC-02(09), AC-03, AC-06(07), AC-21
Administrative Safeguard	Security awareness and training		164.308(a)(5)(i)	AT-01, AT-02, AT-03, AT-04, PM-13
Administrative Safeguard	Security awareness and training		164.308(a)(5)(ii)	AT-02
Administrative Safeguard	Security awareness and training	Security Reminders	164.308(a)(5)(ii)(A)	AT-01, AT-02, AT-03, PM-12, PM-13, PM-16
Administrative Safeguard	Security awareness and training	Protection from Malicious Software	164.308(a)(5)(ii)(B)	AC-04(15), AT-01, AT-02, AT-03, AU-12, IR-08, RA-05, SC-05, SC-10, SC-18, SI-01, SI-02, SI-03, SI-04, SI-08, PM-13
Administrative Safeguard	Security awareness and training	Log-in Monitoring	164.308(a)(5)(ii)(C)	AC-02, AU-02, AU-03, AU-06, AU-10, AU-12, AU-12(03), AU-16(02), CA-07, CM-10, CM-11, IR-08, RA-05, SC-05, PM-13
Administrative Safeguard	Security awareness and training	Password Management	164.308(a)(5)(ii)(D)	IA-02, IA-04, IA-05, IA-06, IA-07, PM-13
Administrative Safeguard	Security incident procedures		164.308(a)(6)	IR-08
Administrative Safeguard	Security incident procedures		164.308(a)(6)(i)	IR-01, IR-02, IR-03, IR-04, IR-07, IR-08, PE-06, PM-15
Administrative Safeguard	Security incident procedures	Response and Reporting	164.308(a)(6)(ii)	AC-21, IR-04, IR-05, IR-06, IR-07, IR-08, RA-05, SI-01, SI-03, SI-04, SI-08, PM-08
Administrative Safeguard	Contingency plan		164.308(a)(7)(i)	CM-03, CM-05, CM-06, CM-07, CM-09, CP-01, CP-02, IR-04(03), PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, SA-10, SC-05, PM-08
Administrative Safeguard	Contingency plan		164.308(a)(7)(ii)	CP-02
Administrative Safeguard	Contingency plan	Data Backup Plan	164.308(a)(7)(ii)(A)	CP-09
Administrative Safeguard	Contingency plan	Disaster Recovery Plan	164.308(a)(7)(ii)(B)	CP-02, CP-06, CP-07, CP-08, CP-09, CP-10, IR-04(03)

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
Administrative Safeguard	Contingency plan	Emergency Mode Operation Plan	164.308(a)(7)(ii)(C)	CP-02, CP-02(05), CP-07, CP-09, CP-10, IR-04(03), PE-10, PE-12, PE-13, PE-14, PE-15, PM-08
Administrative Safeguard	Contingency plan	Testing and Revision Procedures	164.308(a)(7)(ii)(D)	CM-04(02), CP-03, CP-04, PM-06, PM-14
Administrative Safeguard	Contingency plan	Application and Data Criticality	164.308(a)(7)(ii)(E)	CP-02, CP-02(08), PE-09, PE-11, RA-02, SA-05, SA-11, PM-08
Administrative Safeguard	Evaluation		164.308(a)(8)	AU-12, CA-01, CA-02, CA-05, CA-06, CA-07, CA-09, CA-09(01), CM-03, CM-04, CM-04(02), CM-05, CM-06, CM-07, CM-09, IR-08, PL-08, RA-05, SA-05, SA-10, SA-11, SC-05, PM-06, PM-08
Administrative Safeguard	Business Associate contracts and other arrangements		164.308(b)(1)	AC-20, CA-03, PS-07, SA-09, SC-28, PM-01, PM-09, PM-11
Administrative Safeguard	Business Associate contracts and other arrangements	Written Contract or Other Arrangement	164.308(b)(3)	AC-20, CA-03, SA-09
Physical Safeguards	Facility Access Controls		164.310(a)(1)	PE-01, PE-02, PE-02(01), PE-03, PE-04, PE-05, SA-05, SA-11, SC-07, PM-12, PM-16
Physical Safeguards	Facility Access Controls	Contingency Operations	164.310(a)(2)(i)	CP-02, CP-06, CP-07, IR-04(03), PE-09, PE-11, PE-17, SC-05, PM-08
Physical Safeguards	Facility Access Controls	Facility Security Plan	164.310(a)(2)(ii)	PE-01, PE-04, PE-16, PL-02
Physical Safeguards	Facility Access Controls	Access Control and Validation Procedures	164.310(a)(2)(iii)	AC-02(09), AC-03, AC-21, CM-07, MA-01, MA-02, MA-05, PE-01, PE-02, PE-02(01), PE-03, PE-06, PE-08, PE-16, PM-12, PM-16
Physical Safeguards	Facility Access Controls	Maintenance Records	164.310(a)(2)(iv)	MA-01, MA-02, MA-03, MA-05, MA-06, PE-16
Physical Safeguards	Workstation use		164.310(b)	AC-02(09), AC-03, AC-04, AC-11, AC-12, AC-16, AC-16(03), AC-17, AC-17(01), AC-19, AC-20, AC-21, CM-07, PE-02, PE-03, PE-05, PS-06, SC-07
Physical Safeguards	Workstation security		164.310(c)	AC-17, AC-17(01), CM-07, MP-01, MP-02, MP-03, MP-04, PE-02, PE-03, PE-04, PE-05, PE-18, SC-07
Physical Safeguards	Device and media controls		164.310(d)	PM-04, SE-01
Physical Safeguards	Device and media controls		164.310(d)(1)	CA-09, CM-08, MA-04, MP-01, MP-02, MP-03, MP-04, MP-05, MP-06, MP-06(01), MP-07, PE-16, PL-08, SC-28
Physical Safeguards	Device and media controls	Disposal	164.310(d)(2)(i)	MP-06, MP-06(01), MP-07, PE-16, DM-02, DM-02(01)
Physical Safeguards	Device and media controls	Media Reuse	164.310(d)(2)(ii)	MA-04, MP-06

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
Physical Safeguards	Device and media controls	Accountability	164.310(d)(2)(iii)	CM-08, IR-08, MA-01, MA-02, MA-04, MA-05, MP-05, MP-06, PS-06
Physical Safeguards	Device and media controls	Data Backup and Storage	164.310(d)(2)(iv)	CP-09, MP-04, SC-05
Technical Safeguards	Access Control		164.312	AC-04(12), SI-07(06)
Technical Safeguards	Access Control		164.312(a)	AC-06(07)
Technical Safeguards	Access Control		164.312(a)(1)	AC-01, AC-02(09), AC-03, AC-05, AC-06, AC-06(05), AC-11, AC-17, AC-17(01), AC-18, AC-21, CA-03(03), CA-03(05), CA-09, CA-09(01), CM-07, IA-03, IA-06, MA-04, MP-07, SA-05, SA-11, SC-02, SC-04, SC-07, SC-28, PM-12, PM-16
Technical Safeguards	Access Control	Unique User Identification	164.312(a)(2)(i)	AC-02, AC-02(09), AC-03, AC-06(07), AC-14, AC-20, AU-12, CM-07, CM-10, CM-11, IA-02, IA-03, IA-04, IA-08
Technical Safeguards	Access Control	Emergency Access Procedure	164.312(a)(2)(ii)	AC-02, AC-02(09), AC-03, CM-07, CP-02, CP-02(05), IR-04(03), MA-04, PE-09, PE-11, SC-05
Technical Safeguards	Access Control	Automatic Logoff	164.312(a)(2)(iii)	AC-11, AC-12, SC-28
Technical Safeguards	Access Control	Encryption and Decryption	164.312(a)(2)(iv)	AC-02(09), AC-03, AC-17(02), AC-19(05), AU-09(03), CM-03, CM-07, IA-07, MA-04, MP-05(04), MP-07, SC-12, SC-13, SC-28, SC-28(01)
Technical Safeguards	Audit Controls		164.312(b)	AC-06(09), AC-17(01), AC-18, AU-01, AU-02, AU-03, AU-04, AU-06, AU-07, AU-07(01), AU-07(02), AU-09, AU-10, AU-10(01), AU-12, AU-12(03), AU-16(02), CM-10, CM-11, IR-08, MA-04, MP-07, SC-05, SC-07, SC-28
Technical Safeguards	Integrity		164.312(c)	SI-07, SI-07(06)
Technical Safeguards	Integrity		164.312(c)(1)	AC-05, AU-10, AU-10(01), CM-03, CP-09, MP-02, MP-05, MP-06, SA-09, SC-07, SC-08, SC-28, SI-01, SI-07, SI-08(02), PM-12, PM-16
Technical Safeguards	Integrity	Mechanism to Authenticate	164.312(c)(2)	AU-10, AU-10(01), SA-09, SC-08, SC-08(01), SI-07, SI-08(02)
Technical Safeguards	Person or entity authentication		164.312(d)	AU-12, CA-09, CA-09(01), CM-10, CM-11, IA-02, IA-03, IA-04, IA-05, MA-04, MP-06, MP-06(01), SC-28
Technical Safeguards	Transmission Security		164.312(e)(1)	AC-17, AC-17(01), AC-18, AC-20, AU-12, CA-09, CA-09(01), CM-10, CM-11, MA-04, SA-09, SC-07, SC-07(14), SC-08, PM-12, PM-16

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
Technical Safeguards	Transmission Security	Integrity Controls	164.312(e)(2)(i)	AU-10, AU-10(01), AU-12, SA-09, SC-05, SC-07, SC-07(14), SC-08, SC-08(01), SI-07, SI-08(02)
Technical Safeguards	Transmission Security	Encryption	164.312(e)(2)(ii)	AC-17(02), AC-20, CM-03, MA-04, SC-08, SC-12, SC-13, SC-28, SC-28(01)
Organizational	Business Associate Contracts		164.314	AU-16(02)
Organizational	Business Associate Contracts		164.314(a)	AC-20(01), AC-21, PS-06, PS-07, SA-04
Organizational	Business Associate Contracts		164.314(a)(1)	AC-20, PE-09, PE-11, PS-06, PS-07, SA-09, PM-01, PM-08, PM-12, PM-16
Organizational	Business Associate Contracts	Business Associate Contracts	164.314(a)(2)(i)	AC-20, IR-06, IR-08, PS-06, PS-07, RA-05, SA-04, SA-09, PM-04
Organizational	Business Associate Contracts	Other Arrangements	164.314(a)(2)(ii)	AC-20, CA-03, PS-06, PS-07, SA-09
Organizational	Business Associate Contracts	Business Associate Contracts with Subcontractors	164.314(a)(2)(iii)	IR-08, RA-05
Policies and Procedure Documentation Requirements	Policies and Procedures		164.316(a)	PL-01, PL-02, PS-01, RA-01, RA-03, RA-05(05), PM-01, PM-08, PM-09, PM-12, PM-16
Policies and Procedure Documentation Requirements	Documentation		164.316(b)(1)	PL-02
Policies and Procedure Documentation Requirements	Documentation		164.316(b)(1)(i)	PL-01, PL-02, PS-01
Policies and Procedure Documentation Requirements	Documentation		164.316(b)(1)(ii)	CA-01, SI-03(01)
Policies and Procedure Documentation Requirements	Documentation	Time Limit	164.316(b)(2)(i)	AC-20, PL-01, SI-03(01), DM-02
Policies and Procedure Documentation Requirements	Documentation	Availability	164.316(b)(2)(ii)	CA-01, PL-01, PL-02, PS-01

Security Control	Security Standard	Implementation Specification	Reference	Applicable NIST Controls
Policies and Procedure Documentation Requirements	Documentation	Updates	164.316(b)(2)(iii)	CA-06, PE-10, PE-12, PE-13, PE-14, PE-15, PL-01, SA-05, SA-11, PM-06

Appendix E: Security Control Risk Score Formula

Control Risk Rating	
High	7 – 10
Moderate	4 – 6.9
Low	1 – 3.9
Minimal	0

A failed HHS control is rated on a scale from 1 to 10, with 1 being the lowest risk possible for the finding and 10 reflecting the highest possible risk.

Findings with a High-risk score require the Agency Executive Commissioners approval of any risk acceptance/exceptions. The Information Owner, in conjunction with the Agency Information Security Officer can approve risk exception requests for moderate and low-risk.

The finding risk score is calculated using the following formula:

$$Control\ Risk\ Score = \frac{(1 - Control\ Implementation\ Status)x\ ((Control\ Impact - 1)\ x\ 25)}{10}$$

Control Implementation Status:
This variable reflects whether the security control assessed is implemented correctly or not. A control that is not correctly implemented will generate a finding.

- If the control is implemented, this variable equal one (1)
- If the control is not implemented, this variable equals zero (0)

Control Impact
This variable reflects the impact (level of risk) the failure of the control has. There are two variables that make up this control, control score baseline and system score baseline. These variables add together to equal a score between 1 and 5.

$$Control\ Impact = Control\ Score\ Baseline + System\ Score\ Baseline$$

<u>Control Score Baseline</u>
Each security control is assigned a baseline score. This baseline is determined by the following variables. The control score baseline is 40% of the overall impact of a failed security control.

- CIS Critical Control

  - Yes: .75
  - No: 0

- HHS SPI Control
  - Yes: .5
  - No: 0

- NIST Control Priority
  - P1: .5
  - P2: .3
  - P3: .2

- Control Baseline
  - High: .25
  - Moderate: .2
  - Low Plus: .15
  - Low: .10

System Score Baseline

This variable determines the level of risk impact the system poses to HHS. The system score baseline utilizes variables from the HHS system of records, SysCat. The System Score Baseline is 60% of the overall impact of a failed security control.

- System Criticality
  - Mission Critical: .5
  - Not Critical: 0

- System Information Type
  - High (Federally Regulated): 1.5
  - High: 1.25
  - Moderate (Federally Regulated): 1.2
  - Moderate: .95
  - Low Plus: .75
  - Low: .38

- Web Accessibility
  - Employee and Public Access: .5
  - Public Access (Internet): .33
  - Employee Access (Intranet): .25
  - Not on Web: .16

- Number of Users

- Public: .5
- 10,000 or greater: .5
- 5,000 to 9,999: .45
- 1,000 to 4,999: .4
- 100 to 999: .25
- 20 to 99: .175
- 1 to 19: .15
- N/A: .15
- Non-User Interface: .15

Example

AC-02 is not implemented for a **High Baseline**, **Mission Critical**, Intranet/Internet System, **10,000 or Greater** user.

Control Implementation Status = 0

Control Impact = Control Specific Baseline (1.85) + System Specific Baseline (3)

$$Control\ Risk\ Score = \frac{(1-0)x\ ((4.85-1)\ x\ 25)}{10} = 9.625\ (High\ Risk)$$

Appendix F: References and Resources

Texas HHS Legislation, Guidance, and Regulations

Circular C-021*, Information Security/Cybersecurity Policy,* December 22, 2016

Information Security Policy (IS-Policy)*,* v2.0, November 14, 2016

Acceptable Use Policy (HHS-AUP), v1.0, September 25, 2015

Data Classification Standard*,* v3.2, September 30, 2015

Incident Response Framework (IS-IRF), v1.0, August 29, 2016

Incident Response Plan (IS-IRP), v1.0, July 14, 2016

Risk Assessment Monitoring Procedures (IS-RAMP), v1.0, August 31, 2015

Web and Mobile Standard (IS-Web & Mobile), v2.01, September 1, 2017

Security and Privacy Initial Inquiry (SPI), v2.0, January 11, 2016

Acceptable Use Agreement (AUA), v1.0, September 25, 2015

State Legislation, Guidance, and Regulations

Texas Business and Commerce Code Title 11, *Personal Identity Information*, Subtitle B, *Identity Theft*, Chapter 521, *Unauthorized Use of Identifying Information*

Government Code Title 10, *General Government*, Subtitle B, *Information Planning*, Chapter 2054, *Information Resources*

Texas Administrative Code Title 1, *Administration*, Part 10, *Department of Information Resources*, Chapter 202, *Information Security Standards*

Department of Information Resources *Security Controls Standards Catalog*, v1.3, February 26, 2016

Department of Information Resources *Data Classification Guide*, v1.0, March 25, 2014

Federal Legislation, Guidance, and Regulations

The Health Insurance Portability and Accountability Act (HIPAA) of 1996*,* amended March 2013

The Health Information Technology for Economic and Clinical Health (HITECH) of 2009*,* as amended

The Patient Protection and Affordable Care Act, March 23, 2010, 124 Stat. 119

The Social Security Act, as amended

The Privacy Act of 1974, September 27, 1975, 88 Stat. 1896, 5 U.S.C. §552a, as amended

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, ***Security and Privacy Controls for Federal Information Systems and Organizations***, August 2013

NIST SP 800-66 Rev 1, ***An Introductory Resource Guide for Implementing the HIPAA Security Rule***, October 2008

NIST SP 800-63, Version 1.0.2, ***Electronic Authentication Guidelines***, April 2006

NIST SP 800-145, ***The NIST Definition of Cloud Computing*****,** September 2011

NIST SP 800-88 Revision 1, ***Guidelines for Media Sanitization***, December 2014

Federal Information Processing Standards (FIPS) Publication (PUB) 199, ***Standards for Security Categorization of Federal Information and Information Systems***, NIST, February 2004

Internal Revenue Service Publication 1075, ***Tax Information Security Guidelines for Federal, State and Local Agencies and Entities***, September 2016

Office of Management and Budget (OMB), Memorandum M-07-16, ***Safeguarding and Responding to the Breach of Personally Identifiable Information***, May 22, 2007.

Criminal Justice Information Services (CJIS) ***Security Policy,*** v5.6, June 5, 2017

Centers for Medicare & Medicaid Services ***Acceptable Risk Safeguards (ARS)***, v3.0, January 31, 2017

Centers for Medicare & Medicaid Services ***Minimum Acceptable Risk Security and Privacy Controls for Exchanges,*** **Department of Information Resources,** v2.0, November 20, 2015

Center for Disease Controls ***Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs*****,** 2011

Department of Veterans Affairs Handbook 6500, ***Risk Management Framework for VA Information Systems,*** March 10, 2015

Other References

The CIS Critical Security Controls for Effective Cyber Defense, v6.1, August 31, 2016

Definitions

The HHS Information Security Definitions (IS-Definitions) provides the terms used in all HHS Information Security documents. The IS-Definitions document aligns with the Texas Administrative Code (TAC) RULE §202.1 Applicable Terms and Technologies for Information Security Standards and National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, Revision 4 (rev 4) definitions for security terminology.

Attachment G: Information Security Assessment Supplemental Guidance for External Entities

Texas Integrated Eligibility Redesign System (TIERS)
Cloud Assessment and Migration Planning Services
Health and Human Services Commission (HHSC)

TEXAS Health and Human Services

Information Security Assessment Supplemental Guidance for External Entities

Contents

1 Purpose 2
2 Scope 2
3 Definitions 2
4 Guidance 3
4.1 Authority to Receive HHS Data 3
4.2 Complying with HHS Information Security Requirements 4
4.2.1 Security Assessment Report 5
4.2.2 Moderate and High Security Control Baseline Additional Requirements 5
4.2.3 Regulatory or Federal Overlays Additional Requirements 5
4.2.4 Reporting Non-Compliance with HHS Requirements 5
4.3 How to Submit Documentation 6
5 Guidance Documents 7
5.1 Federal and State Laws 7
5.1.1 Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24 7
5.1.2 Information Security Controls (IS-Controls) 7
6 Revision History 7

1 Purpose

This document supplements Texas Health and Human Services' (hereafter referred to as HHS) Information Security Controls (IS-Controls), specifically the following requirements as they apply to external entities:

- CA-02 Security Assessments
- CA-06 Security Authorization
- CA-07 Independent Assessment

This document meets state requirements in Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24, in the Agency Information Security Program. These requirements include protections based on risk for all information and information resources, including resources outsourced to an external entity.

2 Scope

This document affects external entities responsible for complying with the aforementioned HHS information security requirements and HHS employees who are responsible for monitoring external entity compliance.

3 Definitions

Term	Definition
External Entity	Individuals or organizations external to HHS who have an existing or potential contracting relationship that permits the individual or organization to access, create, disclose, receive, transmit, maintain, or store HHS data.
Independent Assessments	Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations.

Term	Definition
Independent Assessor	Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services.

4 Guidance

4.1 Authority to Receive HHS Data

Before an external entity receives HHS data, the external entity must comply with HHS information security requirements as documented in the contractual agreement between the external entity and HHS, and must be authorized to receive data in accordance with IS-Controls CA-06, Security Authorization.

To be granted the authority to connect or authority to operate, the external entity must comply with Section 4.2 Complying with HHS Information Security Requirements.

4.2 Complying with HHS Information Security Requirements

Table 1: Security Compliance Requirements, is an embodiment of IS-Controls CA-02, Security Assessments.[1] An external entity's compliance requirements vary depending on the types of HHS data that it accesses, creates, discloses, receives, transmits, maintains, or stores.

Table 1: Security Compliance Requirements

Security Control Baseline or Overlay[2]	Required Documents	Frequency	Mandated by IS-Controls
Low or Low Plus[3]	Security Assessment Report	Biennial (only submit upon request)	CA-02
Moderate	Security Assessment Report by an Independent Assessor	Biennial	CA-02, CA-02(01)
High	Security Assessment Report by an Independent Assessor	Annual	CA-02, CA-02(01)
IRS, CMS-MARS-E, or CJIS	Security Assessment Report by an Independent Assessor	Annual	CA-02, CA-02(01)

[1] However, an external entity's contractual agreement with HHS may provide more restrictive compliance requirements.

[2] Refer to IS-Controls section 2.1 for a full explanation of all security control baselines and overlays.

[3] HHS requires external entities who must comply with the "low" or "low plus" security baselines to complete a Security Assessment Report on a biennial basis. However, external entities are not required to submit the required documentation to HHS unless otherwise stipulated in the contractual agreement, or unless requested by HHS. If HHS requests the required documentation, the external entity must submit it within 90 days of the request.

4.2.1 Security Assessment Report

The external entity must complete a Security Assessment Report as proof of compliance with HHS information security requirements. In order for HHS to accept the Security Assessment Report, the external entity must do the following:

1. Submit the Security Assessment Report using the HHS template.
2. Attest that the external entity is compliant with all HHS information security controls required per the external entity's contractual agreement with HHS.

4.2.2 Moderate and High Security Control Baseline Additional Requirements

An independent assessment must validate that the external entity meets security compliance requirements. "Independent assessment" is defined in the definition section of this document and described in IS-Controls CA-02(01), Independent Assessors supplemental guidance.

4.2.3 Regulatory or Federal Overlays Additional Requirements

The external entity may receive some data from HHS that originates from another regulatory or federal source that has additional assessment requirements beyond what is mentioned above. The external entity must refer to its contractual agreement with HHS for any added requirements.

4.2.4 Reporting Non-Compliance with HHS Requirements

External entities must submit additional documentation to HHS for each documented instance of non-compliance with HHS information security requirements.

External entities must submit one of the following applicable forms for each instance of non-compliance to document how they will address the reported non-compliance.

4.2.4.1 Plan of Action and Milestone (POA&M) Form

The external entity must complete a separate Plan of Action and Milestone (POA&M) Form for each non-compliant information security control that will be remediated. The external entity must use this form to explain how and when they will become compliant and should include timelines and a remediation plan.

4.2.4.2 Risk Exception Request Form

If the external entity cannot remediate the risk posed by their non-compliance, the external entity must complete a Risk Exception Request Form for each non-compliant information security control that cannot be remediated. The external entity must use the form to explain why they cannot comply with information security requirements and include alternative solutions to reduce the risk posed by the non-compliance.

4.3 How to Submit Documentation

All information security documentation concerning HHS data is classified as confidential. The external entity must send this documentation in a manner compliant with IS-Controls SC-08, Transmission of Confidential Data, and IS-Controls SC-28, Protection of Data at Rest. The external entity should contact the HHS point-of-contact identified in the contractual agreement for further guidance on how to securely submit the documents to HHS.

The external entity must submit a Security Assessment Report, along with any of the following document(s) if applicable:

- POA&M forms
- Risk Exception Request Forms
- Any other required security documentation identified in the contractual agreement

HHS reserves the right to request additional information from the external entity to confirm that the applicable information security requirements are in place.

Failure by the external entity to comply with information security requirements may result in consequences including, but not limited to, liquidated damages, contract termination, regulatory fines, or other remedies.

5 Guidance Documents

The following documents are associated with this guidance.

5.1 Federal and State Laws

5.1.1 Title 1, Part 10, Texas Administrative Code (TAC), Chapter 202, Rule §202.24

Establishes requirements that each agency shall develop, document, and implement an agency-wide information security program that includes protections, based on risk, for all information and information resources.

Link

5.1.2 Information Security Controls (IS-Controls)

Includes safeguards or countermeasures that, when implemented and enforced, satisfy the information security compliance requirements defined in applicable federal and state laws, executive orders, directives, policies, HHS regulations, and standards.

Link

6 Revision History

Date	Change	Department Owner
06/17/2019	Revised and replaced IS-RAMP	Chief Information Security Office
08/31/2015	Issued as IS-RAMP	Chief Information Security Office