Dr. Courtney N. Phillips, Executive Commissioner

STATEMENT OF WORK
Project and Portfolio Management SaaS Configuration & Implementation Services

SOW No. HHS0004417

Date of Release: 10/4/2019
Responses Due: 11/01/2019 by 2p.m. CST

Contents

1. Introduction 5
2. SOW Solicitation Overview 6
2.1. Project Description 6
2.2. SOW Solicitation Point of Contact 6
2.3. SOW Solicitation Schedule 7
2.4. Questions and Answers 7
2.5. SOW Solicitation Contents 7
3. Services Description 8
3.1. Scope of Services 8
3.1.1. Vendor Compliance with Micro Focus SaaS PPM Use Restrictions 8
3.1.2. Objectives of the Services 8
3.1.3. Staged Adoption of SaaS PPM 9
3.1.4. Vendor Suggestions 9
3.1.5. Information Security Requirements 9
3.1.6. TIERS-related Work 9
3.2. Project Period 10
3.3. Project Phases and Deliverables 10
3.4. Additional Project Deliverables 18
3.4.1 Weekly Status Report 18
3.4.2 Issue Log 18
3.4.3 Risk Log 18
4. Deliverables 19
4.1 Deliverables Format 19
4.2 Deliverables Acceptance Criteria 19
4.3 Deliverable Due Dates 19
4.4 Deliverable Review Process 20
4.5 Deliverables Correction 20
4.6 Work Product 20
4.7 Accepted Deliverables – Plans 20
5. Project Changes 20
6. Project Management 21
6.1 Project Schedule 21
6.2 Project Reporting and Tracking 21
6.3 Communication and Meetings 21
6.4 Presentations 21
6.5 Knowledge Transfer 22
6.6 Performance Measures and Associated Remedies 22
7. Invoices 22
8. HHSC/Vendor-Furnished Equipment and Work Space 22
8.1 Restrictions on Access and Use 22
8.2 HHSC Furnished Equipment and Work Space 23
8.3 Vendor Furnished Equipment and Work Space 23
9. Contractor Warranties 23
9.1 General 23

9.2 Warranty Period 24
9.3 Warranty Obligations 24
9.4 HHSC Right of Offset 24
10. Project Termination 24
10.1 For Convenience 24
10.2 Immediate Termination 24
10.3 Notice to Cure 25
10.4 Effect of Termination 25
11. Liability 25
11.1 Acknowledged Direct Damages 25
11.2 Limitation of Liability 26
12. SOW Solicitation Additional Terms and Conditions 26
12.1 Exceptions to Terms 26
12.2 SOW Cancellation and Partial Award or Non-Award 26
12.3 HHSC Right to Reject Proposals or Portions of Proposals 26
12.4 Costs Incurred by Vendors 26
12.5 Incomplete Responses 27
12.6 Property of HHSC 27
12.7 Copyright Restriction 27
12.8 Texas Public Information Act Applicable to Responses 27
12.9 TEC Form 1295 28
13. Response Submission Instructions 28
13.1 Number of Copies 28
13.2 Time and Place of Submission 28
14. Response Organization and Content 29
14.1 Overview 29
14.2 Part 1 – Required Acknowledgments 29
14.3 Part 2 – Qualifications and Background 29
14.4 Part 3 – Technical Proposal 31
14.5 Part 4 – Price Proposal 31
14.6 Exceptions to Terms and Conditions 32
15. Historically Underutilized Business Participation 32
16. Proposal Evaluation 32
16.1 Conformance with State Law 32
16.2 Initial Compliance Screening 32
16.3 Specific Criteria 33
16.4 Questions or Requests for Clarification by HHSC 33
16.5 Oral Presentations and Site Visits 33
16.6 Best and Final Offers 33
16.7 Discussions with Responding Vendors 34
16.8 Award 34
17. Additional Terms and Conditions 34
17.1 External Factors 34
17.2 Standards of Conduct 34
17.3 U.S Department of Homeland Security's E-Verify System 34
17.4 Vendor Due Diligence 35
17.5 Entire Agreement 35

Exhibit A. AFFIRMATIONS AND SOLICITATION ACCEPTANCE 37
Exhibit B: SOW SIGNATURE DOCUMENT FOR 46
4. System Agency 47
5. Contractor 47
SIGNATURE PAGE FOR HHSC STATEMENT OF WORK CONTRACT NO. HHS[xxxxxxxxx] UNDER DIR CONTRACT # DIR-TSO-[xxxx] 49
DIR REVIEW – HHSC SOW ID # HHS[xxxxxx] 49
Exhibit C: HHS Information Security Acceptable Use Policy (HHS AUP): 50
Exhibit D: Health and Human Services Acceptable Use Agreement (AUA): 60
Exhibit E: HHS System Data Use Agreement 69
Exhibit E-1: HHS System Security and Privacy Inquiry (SPI) 82
Exhibit F: Experience Reference Form 101
Exhibit F-1: RESPONDENT RELEASE OF LIABILITY 104
Exhibit G – Vendor Price Sheet 105
Exhibit H – HHSC Uniform Terms and Conditions 108
Exhibit H-1 – HHSC Special Conditions 126
Exhibit I - Scope of Work Supporting Documents 138
Exhibit I-1 – Requirements 139
Exhibit I-2 - User Story Narratives 146
Exhibit I-3: Glossary 173
Exhibit I-4: HHS IT Project Tracking, Time Effort Reporting & Cost Allocation Process 175
Exhibit I-5: Current TIERS PPM Installation Information 194
Exhibit I-6: Other Legacy System Information 196
Exhibit I-7: PPM Production Architecture 199
Exhibit J: FFATA Certification 201
Exhibit K: Certification Regarding Lobbying 204
Exhibit L: Federal Assurances 205
Exhibit M: FNS Handbook 901 Federal Procurement Clauses 208
Exhibit N: Insurance Requirements HHS0004417 Project and Portfolio Management Configuration & Implementation Services 212

1. Introduction

The State of Texas (the "**State**") Health and Human Services Commission ("**HHSC**") is the state agency that administers and/or provides health and human services in the State, through the health and human services system (the "**HHS System**"). As set forth in Texas Government Code, Chapter 531, the HHS System refers to all HHSC offices and divisions and any other governmental entity that is under the administrative and operational control of the Executive Commissioner of HHSC. The Department of State Health Services ("**DSHS**") is a separate Texas agency that is under the administration of HHSC and is thus part of the HHS System.

HHSC has prepared this Statement of Work ("**SOW**") Solicitation to engage a single qualified vendor (the "**Vendor**," "**Contractor**," or "**Respondent**") to install, configure, and implement the Micro Focus Project and Portfolio Management ("**PPM**") Software-as-a-Service (SaaS) solution across the HHSC user groups. HHSC currently uses six (6) different tools for cost and resource allocation and demand management, all of which are implemented as installed software managed by HHSC and/or its vendor(s). One of those tools is the Micro Focus PPM solution; the remaining five (5) tools are various third-party proprietary products and HHSC-custom-developed tools. HHSC seeks conversion, migration, configuration, and implementation services to expand HHSC's use of the Micro Focus PPM platform to convert data and users from the legacy tools as well as to upgrade and migrate the existing instance of Micro Focus PPM to the current version of Micro Focus SaaS PPM. Micro Focus SaaS PPM is a proprietary product owned by Micro Focus International plc. Vendor must have full permission and all necessary intellectual property rights and license from Micro Focus to perform the Services described herein. Procurement of the Micro Focus SaaS PPM solution and decommissioning of the HHSC legacy tools are not included in the scope of Services for this engagement.

In addition to the conversion and migration of the existing legacy databases and workflows, the selected Vendor will configure and implement the specified features and functionality of the Micro Focus SaaS PPM tool as described in the project details below. The desired outcome is seamless and integrated resource management and time allocation functions across all HHSC user groups using the Micro Focus SaaS PPM solution. HHSC's current implementation of the Micro Focus PPM software is integrated with HHSC's Texas Integrated Eligibility Redesign System (TIERS) environment. TIERS-related use of the Micro Focus PPM tool accounts for approximately eighty percent (80%) of the data and use within the current PPM implementation. The remaining twenty percent (20%) is associated with non-TIERS users in HHSC's IT division. This implementation of PPM includes customizations specific to the TIERS users, as well as several complex and large TIERS-related workflows that must be accurately re-configured and implemented in the Micro Focus SaaS PPM instance. HHSC TIERS personnel have reviewed the Micro Focus SaaS migration tool and believe that the Micro Focus migration tool will migrate the existing implementation, including all of the TIERS customizations and workflows, successfully, following which the Vendor will configure the migrated instance to restore feature/functionality rather than re-creating the feature/functionality as a new implementation. As further described in **Section 3.1.5** below, **TIERS-related Work**, HHSC may opt to proceed without the TIERS-related Work in the scope of Services. In the event that HHSC awards this SOW Solicitation with the TIERS-related Work included, HHSC reserves the right to remove the TIERS-related Work from the scope of Services, in the sole discretion of HHSC, at any time upon written notice to the selected Vendor, and any such reduction in scope of Services shall result in an automatic equitable reduction of the costs payable to the selected Vendor.

This SOW is authorized by and in compliance with the provisions of Texas Government Code Chapters 531, 2155 and 2157. HHSC in its sole discretion may elect to award all or part or none of the Work described by this SOW. Each prospective Vendor must be under a current contract with the Texas

Department of Information Resources ("**DIR**") that allows the Vendor to provide the services described in this SOW to HHSC (the "**DIR Contract**"). 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. HHSC will only consider Vendors for this SOW who have current agreements with DIR and who are permitted under their respective DIR contracts to deliver the services described by this SOW. HHSC reserves the right to modify or amend this SOW at any time prior to execution of a final contract between the successful Vendor and HHSC (the "**Contract**"). Refer to **Appendix A** of Vendor's DIR Contract, **Exhibit H** of this SOW, **HHSC Uniform Terms and Conditions**, and **Exhibit H-1** of this SOW, **HHSC Special Conditions**, for defined terms in addition to those defined herein.

2. SOW Solicitation Overview

2.1. Project Description

HHSC has selected the Micro Focus SaaS PPM solution as HHSC's desired project and portfolio management tool. Currently, there is no centralized solution where project information (schedules, budgets, risks and issues, etc.) or asset portfolios can be accessed, reviewed, and analyzed by stakeholders. HHSC will submit this SOW for a Response to a minimum of six (6) qualified vendors under DIR cooperative contracts. HHSC seeks a qualified information technology ("**IT**") services provider to implement and configure the SaaS PPM tool as a deliverables-based engagement that is required to be completed within twenty-four (24) months from the Effective Date of the Contract (as defined in the **SOW Signature Document**, attached hereto as **Exhibit B**). The twenty-four month time frame given above is inclusive of three (3) months estimated for completion of required background checks for Vendor personnel working under the SOW, therefore prospective Vendors should account for this contingency in their proposed work plans and schedules. **Section 10, Subparagraph J** of **Appendix A** of the DIR Contract will govern HHSC's and Contractor's rights and obligations with respect to the performance of background checks of Contractor personnel.

Due to funding constraints applicable to state agencies, Vendor agrees that time is of the essence for Vendor's timely completion of the services described by this SOW (the "**Services**"), including completion of the project deliverables described below (the "**Deliverables**"). HHSC will provide a single point of contact for all communications and management of Vendor's work under this SOW (the "**HHSC Project Manager**"). If requested by the HHSC Project Manager, Vendor will perform work outside of regular business hours, including after-hours and on weekends, as needed to ensure timely completion of the Services and/or to complete tasks that cannot be performed during regular business hours. Unless specifically permitted otherwise by the HHSC Project Manager, all Services will be performed on-site at HHSC offices and using laptops and desktops provided by HHSC. Vendor will perform all work at 4900 N. Lamar Blvd., Austin, TX 78751 or remotely at HHSC's discretion. This SOW does not include reimbursable travel expenses.

HHSC has included **Exhibit I** to this SOW that describes the requirements, user stories, and other information for prospective Vendors' reference in developing their responses to this SOW Solicitation ("**Responses**").

2.2. SOW Solicitation Point of Contact

The sole point of contact for inquiries concerning this SOW is:

Health & Human Services Commission
Procurement and Contract Services
Brad Westbrook, CTCD, CTCM
1100 W 49th Street
Austin TX 78756
MC 2020
512-406-2557

All communications relating to this SOW must be directed to the HHSC point of contact named above (the "**HHSC Point of Contact**"). All communications between Vendors and other HHSC staff members concerning this SOW are strictly prohibited. **A Vendor's failure to comply with these requirements may, in HHSC's sole discretion, result in that Vendor's disqualification from this SOW solicitation.**

2.3. SOW Solicitation Schedule

The following dates represent HHSC's desired schedule of events associated with this SOW inquiry. HHSC reserves the right to modify these dates at any time. All times stated in this SOW are given in Central Standard Time.

Date	Activity
October 4, 2019	Distribute SOW to prospective vendors
October 11, 2019 [2 pm]	Vendor deadline for submitting questions to HHSC
October 18, 2019	Anticipated HHSC response to questions
November 1, 2019 [2 pm]	Vendor deadline for submitting responses to SOW
December 13, 2019	Anticipated award
January 10, 2020	DIR review completed
March 6, 2020	Federal review completed
March 10-16, 2020	HHSC contract signing
March 23, 2020	Project start

2.4. Questions and Answers

Vendors must submit all questions regarding this SOW by email to the HHSC Point of Contact. Questions regarding this SOW will be accepted by the HHSC Point of Contact until the date and time specified in the table above.

By submission of a question, Vendor acknowledges that the applicable question and official answer may be shared with other Vendors and therefore Vendors will not include any confidential or proprietary information in such questions. HHSC will not identify by name the Vendor that submitted any particular question.

2.5. SOW Solicitation Contents

This SOW consists of these terms and conditions and the following exhibits, each of which is attached hereto and incorporated into this SOW by this reference:

Exhibit A: Contract Affirmations and Solicitation Acceptance;
Exhibit B: Form of SOW Signature Document;
Exhibit C: HHS Information Security Acceptable Use Policy (HHS AUP);
Exhibit D: Health and Human Services Acceptable Use Agreement (AUA);
Exhibit E: HHS Data Use Agreement ver. 8.5;
Exhibit E-1: HHS Security and Privacy Inquiry (SPI);
Exhibit F: Experience Reference Form;
Exhibit F-1: Respondent Release of Liability;
Exhibit G: Vendor Price Sheet;
Exhibit H: HHSC Uniform Terms and Conditions;
Exhibit H-1: HHSC Special Conditions;
Exhibit I: Scope of Work Supporting Documents;
Exhibit I-1: Requirements;
Exhibit I-2: User Story Narratives;
Exhibit I-3: Glossary;
Exhibit I-4: HHS IT Project Tracking, Time Effort Reporting & Cost Allocation;
Exhibit I-5: Current PPM Installation Information;
Exhibit I-6: Other Legacy System Information;
Exhibit I-7: PPM Production Architecture;
Exhibit J: FFATA Certification;
Exhibit K: Certification Regarding Lobbying;
Exhibit L: Federal Assurances; and
Exhibit M: FNS Handbook 901 Federal Procurement Clauses; and
Exhibit N: Insurance Requirements.

By submitting a response to this SOW Solicitation ("**Response**"), the responding Vendor is making a binding offer to contract with HHSC based upon the terms, conditions, specifications, representations and warranties contained in: i) this SOW, ii) the DIR Contract, and iii) the Vendor's Response. Offers from vendors do not become contracts with HHSC unless, and only to the extent, the duly authorized representatives of Vendor, HHSC, and DIR execute the SOW Signature Document incorporating this SOW and its exhibits and other listed contract attachments (collectively, the "**Contract**").

3. Services Description

3.1. Scope of Services

3.1.1. Vendor Compliance with Micro Focus SaaS PPM Use Restrictions

Procurement of the SaaS PPM tool is out of scope for this engagement. However, Vendor is required to adhere to the use restrictions of the HHSC SaaS PPM services subscription agreement with Micro Focus, and to advise HHSC if Vendor believes that the scope of use of the SaaS PPM solution purchased by HHSC is insufficient to complete the Services.

3.1.2. Objectives of the Services

HHSC desires the SaaS PPM tool to be configured in a manner that aligns with the HHSC project management and governance models, including both waterfall and agile project methodologies, and to optimize the decision-making and performance measurement features of the SaaS PPM tool for HHSC's particular technical, financial, compliance, resource, and governance requirements. Specifically, the

configuration will include the portfolio intake and business case workflow management, demand management, time tracking, resource capacity planning, program management and road mapping, project budget management, project records management, and a customizable dashboard that drives strategic and tactical, evidence-based decisions. In addition, Vendor will configure and implement the SaaS PPM solution to accommodate and preserve, to the maximum extent available, existing workflows used by the various HHSC user groups. Vendor will proactively communicate to the HHSC Project Manager any gaps in reproducing existing workflows in the SaaS PPM solution and propose mitigation and workaround strategies to meet the business and operational requirements as fulfilled by the legacy workflow.

3.1.3. Staged Adoption of SaaS PPM

Vendor will work closely with the HHSC project team and internal stakeholders to understand the legacy environments from a technical, operational, and strategic business perspective. On the basis of the information obtained from stakeholders and provided in this SOW, Vendor will perform the Services in strategically defined stages to minimize user and business process disruption while optimizing adoption of the features and functionality of the Micro Focus SaaS PPM solution. Vendor will perform this staged adoption across the Health and Human Services system through established strategic application portfolios and at the program business unit level, to facilitate HHSC's realization of intended investment benefits from the Micro Focus SaaS PPM solution.

3.1.4. Vendor Suggestions

Although this SOW has been written prescriptively with a high level of detailed requirements, HHSC is also open to recommendations from prospective Vendors for project definition and approach. This SOW is intended to provide prospective Vendors the right balance of detail and insight into the scope, objectives, and intended project outcomes. This should enable prospective Vendors to provide HHSC with a high-quality Response describing in detail how their business and technical expertise and the on-point experience of their proposed team will enable the successful implementation of the HHSC SaaS PPM platform on time and on budget.

3.1.5. Information Security Requirements

Vendor's obligations with respect to information security requirements are twofold. As the Vendor performing the Services, Vendor is subject to the confidentiality obligations of the Contract. HHSC advises Vendor that the current TIERS PPM implementation includes PHI, PII, SPI, and Social Security Administration Data, as those are defined in the **Data Use Agreement** attached as **Exhibit E** to this SOW. Legacy systems include PII. In addition, in the course of performing the Services, Vendor will assess, configure, and implement the application-level information security requirements for the HHSC SaaS PPM implementation in accordance with the requirements provided by HHSC. In the event that the SaaS PPM application is unable to be configured to meet the information security requirements of HHSC, Vendor will advise HHSC and consult with HHSC data owners in mitigating or adjusting HHSC's use of the SaaS PPM tool to address any such gaps. Finally, Vendor's knowledge transfer documentation will specifically address the information security settings configured and implemented by Vendor in the Micro Focus SaaS PPM.

3.1.6. TIERS-related Work

HHSC may include or exclude work related to the HHSC TIERS implementation of Micro Focus SaaS

PPM in any contract resulting from this SOW Solicitation. The TIERS-related work in this SOW is the work that refers to migration of the TIERS data and users in the current PPM implementation to the Micro Focus SaaS PPM instance (the non-TIERS use of the current implementation does not include the customizations or workflows used by the TIERS users). HHSC TIERS personnel have completed the Micro Focus questionnaire for migration of the current PPM implementation into the Micro Focus SaaS PPM environment. The TIERS implementation of SaaS PPM may require application-level security configurations and settings such that it may be necessary to configure a separately partitioned TIERS SaaS PPM instance. In addition, the current TIERS PPM on-prem implementation relies heavily on use of the PPM Demand Management module. It is anticipated that this reliance on the Demand Management tools within Micro Focus SaaS PPM will continue in the SaaS PPM TIERS implementation, and also that the TIERS SaaS PPM instance will be configured to support TIERS personnel to increase their leverage and use of the resource management features of the SaaS PPM tool. In addition to the foregoing, HHSC has identified the following activities and requirements as within scope to the TIERS-related Work:

1) **Section 3.3**, Phase I: activity commented as including "TIERS"
2) **Exhibit I-1**: Requirement IDs B01.016, B01.017, and B03.014
3) **Exhibit I-2**: Three User Story Narratives marked as "(TIERS)"
4) All other references to the "current PPM implementations," to the extent those relate to the TIERS-related use of the current PPM implementation.

When completing their Responses, prospective Vendors should refer to the above list in determining impact to cost and schedule to perform the TIERS-related Work. Accordingly, the **Vendor Price Sheet** set forth at **Exhibit G** of this SOW provides space for prospective Vendors to specify their proposed pricing for the Services that are attributable solely to performance of the Services that comprise the TIERS-related Work. HHSC will rely on this amount as the amount that would be ***excluded*** from the Vendor's proposed pricing in the event that HHSC opts to proceed with this SOW without including the TIERS-related Work in the scope of Services. Prospective Vendors should also indicate in their proposed work schedules any impact to the proposed time periods if HHSC opts not to include the TIERS-related Work in the scope of Services. To summarize, Prospective Vendors should submit their proposals for the full scope of Services described by this SOW but should specify the impacts to pricing and schedule if HHSC opts not to include the TIERS-related Work in the scope of Services for the awarded contract. ***By submitting a Response to this SOW Solicitation, Vendors are submitting a binding offer to perform the Services with or without the TIERS-related Work included in the scope of Services.***

3.2. Project Period

Vendor is required to complete the Services over a contiguous twenty-four (24) month term, commencing on the Contract Effective Date. HHSC in its sole discretion may elect to renew and extend the Contract for up to two (2) one-year renewal terms. Adherence to the Project Schedule (as defined below in **Section 4.3**) is a material obligation of Vendor under this SOW. HHSC may require Contractor to provide some after-hours and weekend work to complete tasks that cannot be accomplished during regular business hours. Such after hours and weekend work shall not incur additional charges or fees except as may be set forth in the Contract.

3.3. Project Phases and Deliverables

Vendor will perform the Services using a phased approach, as generally described below. In completing each of the phases, Vendor will configure and implement the SaaS PPM instance(s) to incorporate and meet the applicable requirements and specifications given in the documentation provided in **Exhibit I**. The Project Schedule (defined below in **Section 4.3**) indicates when each of the project phases and Deliverables are to be completed. During Phase 1, Vendor will develop the strategy for conversion of

legacy systems and migration of the current PPM implementation, including both the TIERS users and the non-TIERS users, to the SaaS PPM instance. Because the current PPM system does not require conversion, Vendor may wish to isolate the migration of the current PPM to the SaaS PPM into a separate task that may be executed during a later phase of the Project. The Vendor will develop the optimal work plan and order of activities for the SaaS PPM implementation in a collaborative process involving the HHSC Project Manager and the various internal stakeholders for each of the legacy systems.

Phase 1 - Implement Time Management, Resource Management, Project Management, Demand Management & Portfolio Management

Contractor's Phase 1 tasks include:

- Verify and prioritize the requirements and user stories set forth in **Exhibit I**
- Create requirements traceability matrix from **Exhibit I**; reflect the configuration/implementation of each of the requirements and the appropriate phase
- Develop and define PPM implementation roadmap, including constraints
- Develop communication plan to address all phases of the project; should include Vendor's escalation strategy
- Develop knowledge transfer plan to address all phases of the project
- Identify historical information for conversion for each legacy system following HHSC records retention requirements contained in **Exhibit I-1**.
- Develop a detailed project work plan
- Provide portfolio management process discovery and design
- Provide PPM application infrastructure/installation support for non-production
- Provide PPM application infrastructure/installation support for production
- Provide administrative configuration setup
- Provide work item definition and related process design
- Provide resource management process discovery and design
- Provide cost related process discovery and design
- Provide time management process discovery and design
- Provide demand management process discovery and design
- Implement work item and related process configuration
- Implement resource management
- Implement cost allocation
- Implement time management
- Implement portfolio management
- Implement demand management (all of IT uses this module, but TIERS relies on it heavily: 80+ requests, 130+ workflows, legacy projects, etc.)
- Implement reports development
- Provide end to end solution testing
- Provide system integration testing
- Provide end user testing
- Develop conversion plan for legacy data from Dovico, SalesForce, BASS OIG-IT time reporting applications, FY (Fiscal Year Planning) and PMRS (Project Management Reporting System)
- Develop migration plan for legacy data and functionality from existing PPM installation (includes both non-TIERS IT users and TIERS users)
- Ensure conversion and implementation of existing two-way interface with remedy on demand
- Develop user training plan

- Develop training for administrators
- Develop training for operators/users
- Provide rollout and post rollout support
- Implement mobile web client using web browser for remote time reporting (should not access any of the HIPAA data contained in project files)
- Perform load testing on the PPM application
- Work with HHSC Application Development Security project team members to insure security control compliance

As part of Phase 1, Vendor will complete the following Deliverables:

Deliverable No.	Deliverable	Deliverable Description
D.1.1	Project Work Plan	A work breakdown structure (WBS) encompassing the entire scope of the SOW. This deliverable is a revised version of the project work plan included with Vendor's Response. Following acceptance of the Project Work Plan by HHSC, the Project Work Plan supersedes the work plan included in the Vendor's Response. Vendor will continually maintain and update the Project Work Plan as needed to reflect work progress to-date. WBS should include the resources by name & function, assignments to task and hours per individual by task.
D1.2	Communication Plan & Escalation Strategy	Detail communications between Vendor and HHSC, how issues will be tracked, mitigated and escalated. The escalation chain needs to be identified and defined.
D1.3	Knowledge Transfer Plan	Document the "as is" functionality, update to reflect the "to be" future, update the existing architectural documents.
D1.4	PPM Installation Checklist	Provide process planned to implement new version of PPM
D1.5	PPM Configuration Documentation and updates throughout project	The current state of the environment is to be updated /documented throughout the project.
D1.6	Functional Design (Word/Excel)	High-level description of inputs, process outputs and processes (modules performing those tasks) including the planned configuration parameters and settings.
D1.7	Process Workflows (Visio)	Diagram of complete system functionality reflecting both existing and new.

Deliverable No.	Deliverable	Deliverable Description
D1.8	Requirements and User Stories	Verified and corrected/completed requirements and user stories set forth at Exhibit I-1 and Exhibit I-2 and mapped to PPM module and Project Phase.
D1.9	End User Testing Acceptance	Acceptance by all user groups to verify solution is working correctly and items needing remediation have been corrected
D1.10	Migration Plan	Provide detail on the moving of the existing PPM system to the new PPM system including the RoD interface functionality with planned migration dry runs and validation activities. (includes both non-TIERS IT users and TIERS users)
D1.11	Conversion Plan	Provide detail mapping of data elements from non-PPM legacy systems. Provide information on how the data will be extracted, translated and loaded (ETL) into the new PPM environment with planned migration dry runs and validation activities.
D1.12	Converted data into PPM from Dovico, Salesforce & BASS OIG-IT time reporting applications	Verify that ETL data is complete and accurate.
D1.13	Migrated data into PPM from FY (Fiscal Year) Planning and PMRS (Project Management Reporting System)	Verify that extracted and loaded data is complete and accurate.
D1.14	Requirements Traceability Matrix	Verified requirements tested against the Requirements Traceability Matrix
D1.15	Training Plan	Create plan of training including who to be trained, how training will occur, length of training, where training will occur, documents/tools to be created
D1.16	Administrator Training Package	Create a complete document for the administrator(s) for all functionality implemented
D1.17	Operator/User Training Package	Create a user training document that reflects the implemented functionality
D1.18	Mobile time reporting (phone or tablet)	Provide training to subset of users on use of mobile time reporting
D1.19	Load Testing	Successful Load Testing results containing transactions and concurrent users providing the same level or better of service as in current environment

Deliverable No.	Deliverable	Deliverable Description
D1.20	Security Compliance	Work with HHSC to validate the new implementation/configuration has not compromised security compliance
D1.21	Phase Closeout	Assessment of the phase to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the phase has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted.
D1.22	TIERS Related Work	Specifically identified tasks related to TIERS existing or future requirements verified during the completion of the verification of requirements and user stories.

Phase 2 - Interfaces

Contractor's Phase 2 tasks include:

- Design and development of a one-way interface for CAPPS to feed into PPM
- Provide plug-in or 2-way interface for MS Project
- Design and development of one-way interface for PPM audit logs to feed into Splunk
- Update the requirements traceability matrix
- Provide utility to maintain only the data required as defined by the records retention schedule defined in the Requirements in **Exhibit I**.
- Perform load testing on the PPM application.
- Work with HHSC Application Development Security project team members to ensure security control compliance

As part of Phase 2, Contractor will complete the following Deliverables:

Deliverable No.	Deliverable	Deliverable Description
D2.1	Requirements Traceability Matrix	Update Requirements Traceability Matrix created in Phase 1 with tasks completed performed in Phase 2
D2.2	One-way interface for CAPPS to feed into PPM	Nightly batch job to load new, terminated and changed employee data
D2.3	One-way interface for PPM audit logs to feed into Splunk	Audit logs to be exported in a timely basis (as determined during requirements verification) into the Splunk application database
D2.4	System Integration Testing (SIT)	Successful SIT results reviewed and accepted by HHSC project staff
D2.5	End to End (E2E) Solution Testing	Successful E2E results reviewed and accepted by HHSC project staff

Deliverable No.	Deliverable	Deliverable Description
D2.6	Load Testing	Successful Load Testing results containing transactions and concurrent users providing the same level or better of service as in current environment
D2.7	Security Compliance	Work with HHSC to validate the new implementation/configuration has not compromised security compliance
D2.8	End User Testing	Acceptance by all user groups to verify solution is working correctly and items needing remediation have been corrected
D2.9	Utility to remove the records no longer required as defined by the HHSC records retention requirements listed in **Exhibit I-1**.	Create, document and test utility to comply with records retention limits defined in **Exhibit I-1**
D2.10	Plug-in for MS Project	Provide training on use of MS Project plugin
D2.11	Phase closeout	Assessment of the phase to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the phase has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted.
D2.12	TIERS Related Work	Specifically identified tasks related to TIERS existing or future requirements verified during the completion of the verification of requirements and user stories.

Phase 3 - Implement Program and Financial Management.
Contractor will provide:

- Provide program related process discovery and design
- Provide financial management process discovery and design
- Update the requirements traceability matrix
- Implement program management
- Implement financial management
- Provide reports development
- Provide end to end solution testing
- Provide system integration testing
- Support end user testing
- Update training for administrators
- Update training for operators/users
- Provide rollout and post rollout support

- Complete project closeout phase review

Contractor will produce these deliverables:

Deliverable No.	Deliverable	Deliverable Description
D3.1	PPM Configuration Documentation and updates throughout project	Updated environment document.
D3.2	Updated PPM Installation Checklist	Provide process planned to implement new modules of PPM implemented in this phase
D3.3	Functional Design (Word/Excel)	High-level description of inputs, process outputs and processes (modules performing those tasks)
D3.4	Process Workflows (Visio)	Diagram of complete system functionality reflecting both existing and new.
D3.5	Updated Requirements Traceability Matrix	Verified requirements tested against the Requirements Traceability Matrix
D3.6	End User Testing Acceptance	Acceptance by all user groups to verify solution is working correctly and items needing remediation have been corrected
D3.7	Administrator Training Package	Create a complete document for the administrator(s) for all functionality implemented
D3.8	End User Training Package	Create a user training document that reflects the implemented functionality
D3.9	System Integration Testing	Successful SIT results reviewed and accepted by HHSC project staff
D3.10	End to End Testing	Successful E2E results reviewed and accepted by HHSC project staff
D3.11	Load Testing	Successful Load Testing results containing transactions and concurrent users providing the same level or better of service as in current environment
D3.12	Security Compliance	Work with HHSC to validate the new implementation/configuration has not compromised security compliance

Deliverable No.	Deliverable	Deliverable Description
D3.13	Phase Closeout	Assessment of the phase to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the phase has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted. and everyone agrees to final signoff on open contracts
D3.14	TIERS Related Work	Specifically identified tasks related to TIERS existing or future requirements verified during the completion of the verification of requirements and user stories.

Phase 4 - Custom Reports

Contractor will provide:

- Reports development (20)
- Update the requirements traceability matrix

Contractor will produce these deliverables:

Deliverable No.	Deliverable	Deliverable Description
D4.1	Reports (20 custom reports)	Create, test, verify report results for 20 custom reports
D4.2	Updated Requirements Traceability Matrix	Verified requirements tested against the Requirements Traceability Matrix
D4.3	Phase/Project Closeout	Assessment of the phase to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the phase has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted, and everyone agrees to final signoff on open contracts
D4.4	TIERS Related Work	Specifically identified tasks related to TIERS existing or future requirements verified during the completion of the verification of requirements and user stories.

3.4. Additional Project Deliverables

3.4.1 Weekly Status Report

On every Monday (or the first business day of the week if Monday is a state holiday) prior to 5:00 p.m., Vendor will submit a written status report to the HHSC Project Manager that will describe for the prior week: tasks and activities completed, Deliverables submitted to HHSC for review, Deliverables in progress, Deliverables not yet started, activities under way, issues needing to be addressed, issues resolved during the week. Deliverables identified for the weekly status report should only include one project phase at a time, unless otherwise requested by the HHSC Project Manager. The weekly status report will also include the current Issue Log, Risk Log and the Project Work Plan.

3.4.2 Issue Log

Throughout the duration of the Contract, Vendor will maintain and update on a daily basis an Issue Log (as defined herein). Vendor will deliver the current Issue Log to the HHSC Project Manager with the weekly status report, and more frequently as may be requested by HHSC. Vendor's Issue Log will contain a dashboard detailing issues for the Deliverables and the Project indicating a Red, Yellow, or Green status (as defined below) for each Deliverable or issue that will delay the project as a whole.

- **Green (G)** - Deliverable is on schedule for delivery by due date. No known issues exist.
- **Yellow (Y) -** Deliverable is on schedule for delivery by due date, but there are potential issues that could affect the timely completion of the deliverable and these issues are being monitored by Vendor.
- **Red (R)** - the Deliverable is not on schedule for delivery by due date; corrective action by Vendor is required.

Vendor will provide, for any Deliverable whose status is Yellow, a detailed issue mitigation strategy that fully addresses all known issues. Vendor will provide, for any Deliverable whose status is **Red**, a detailed corrective action plan to get the Deliverable back on schedule. **Vendor will provide a daily update for any Deliverable whose status is Red until Vendor returns the status to Yellow or Green**.

In the event of a disagreement between HHSC and Vendor as to the designation of any Deliverable as Green, Yellow, or Red, Vendor will adopt the preferred issue designation of HHSC.

3.4.3 Risk Log

Throughout the duration of Vendor's performance hereunder, Vendor will maintain and update on a daily basis a Risk Log (as defined herein). Vendor will deliver the current Risk Log to the HHSC Project Manager with the weekly status report, and more frequently as may be requested by HHSC. Vendor's Risk Log will contain a table detailing potential risks for the project. Risks are defined as potential events or actions that could impact the Project Schedule, scope or budget. The Risk Log will specify, for each identified risk, the project constraint/constraints (schedule, scope, or budget) that are potentially impacted by the risk, the likelihood of the risk, the magnitude rank of the risk, the risk owner, preventive actions to avoid the risk, and contingency actions to take in the event the risk materializes. Examples of risks include: changes to personnel, HHSC sponsor executive leadership change, errors in time estimates, activities missing from scope, dependencies are inaccurate, information security incidents occur, etc.

Vendor will provide a detailed risk prevention strategy that fully addresses each potential risk to the project. The risks will be monitored on a weekly basis. If the risk has materialized, the item will be moved from the Risk Log to the Issue Log.

In the event of a disagreement between HHSC and Vendor as to whether the risk has moved to the issue category, the Vendor will adopt the preferred risk or issue designation of HHSC.

4. Deliverables

4.1 Deliverables Format

Vendor will submit all Deliverables in a format approved by the HHSC designated point of contact. Microsoft Office 2013 or newer is required. Guidelines for approved format are:

a. Schedules and Timelines - both a Microsoft Project file and a PDF version;
b. Documents - Microsoft Word;
c. Spreadsheets - Microsoft Excel; and
d. Diagrams - Microsoft Excel, Visio, Project or other agreed-to editable formats. Microsoft Visio object may be embedded in a Microsoft Word document. These files will not be password protected.

4.2 Deliverables Acceptance Criteria

HHSC will apply the following acceptance criteria (the "**Acceptance Criteria**") in HHSC's review of submitted Deliverables for conformance with the requirements of this SOW. HHSC may add additional acceptance criteria to those stated below in its sole discretion by advising Vendor in writing of the additional acceptance criteria.

a. Deliverables must be submitted on time.
b. Deliverables are to be submitted to the HHSC Project Manager and appropriate HHSC staff in a deliverable walk-through meeting. The HHSC Project Manager will determine the appropriate staff to be present in each deliverable walk-through.
c. Narrative Deliverables must be presented in terms and language so that a non-technical person may understand them.
d. Deliverables must meet all applicable requirements and specifications set forth in **Exhibit I**, as verified and corrected/completed by deliverable D1.8.
e. Deliverables must meet all applicable requirements and specifications set forth in the project documents created by Vendor through the course of performance of the Services or otherwise provided by HHSC to Vendor.
f. Deliverables must be provided in an HHSC approved format, created using the software as described in **Section 4.1**, **Deliverables Format**, above.
g. Deliverables must meet the criteria provided for each Deliverable in **Section 3**, above.
h. Deliverables must meet all other applicable criteria set forth in the DIR Contract and this SOW.
i. Deliverables must be in compliance with HHSC Accessibility guidelines (https://accessibility.hhs.texas.gov/policy.htm).

4.3 Deliverable Due Dates

Vendor will complete Deliverables by the dates specified in the Project Schedule proposed by Vendor and included in its Response, referred to hereafter as the "**Project Schedule**." Vendor will include in its proposed Project Schedule sufficient interims between the due dates of Deliverables: i) to provide HHSC with adequate visibility into Vendor's activity progress, and ii) to allow for HHSC to complete the

Deliverable approval process described below, including the potential requirement for Vendor to re-work Deliverables.

4.4 Deliverable Review Process

A Deliverable is not considered "complete" and accepted by HHSC until HHSC has reviewed and approved the Deliverable according to HHSC's internal process requirements. HHSC will make reasonable efforts to complete its review of each submitted Deliverable within ten (10) business days or as otherwise mutually agreed by the Parties in writing. The ten (10) business day review period begins at the completion of the Deliverable walk-though meeting with HHSC staff.

4.5 Deliverables Correction

If HHSC determines a Deliverable does not meet the Acceptance Criteria (a "**Defective**" Deliverable), the HHSC Project Manager will advise Vendor of the specific reason(s) for the rejection of the Deliverable, and the Vendor will have five (5) business days from HHSC's rejection to correct the Deliverable and resubmit the Deliverable to HHSC for review. Upon resubmission and following an updated Deliverable walk-through meeting of the changes made, HHSC will use reasonable efforts to review the corrected Deliverable within five (5) business days following the Deliverable walk-through meeting. If HHSC rejects a Deliverable a second time, HHSC may, at its option and sole discretion, either terminate this SOW for cause upon written notification to Vendor or provide Vendor an additional five- (5-) day period to correct and resubmit the Deliverable. This cycle of re-submission and review will continue until either (i) HHSC has approved the Deliverable, or (ii) HHSC has terminated this SOW for cause.

Vendor will not charge HHSC for the costs of performing any rework or correction of rejected Deliverables. The Vendor will perform rework of rejected Deliverables without adverse impact to the Project Schedule, including adding additional resources as needed to perform the Services.

4.6 Work Product

As used herein, "**Work Product**" has the meaning given in the DIR Contract, and additionally includes documents, diagrams, work plans, work-in-progress, meeting minutes, interview notes, and other artifacts created by Vendor as ancillary to the Deliverables, but which are not Deliverables subject to the acceptance process. Any and all Work Product generated by Vendor during the course of and pertaining to this project will be provided to and be the sole property of HHSC. Vendor will surrender all Work Product to HHSC prior to the termination or expiration of this SOW. With respect to Vendor IP or Third Party IP, as defined in the DIR Contract, that is included in Work Product, HHSC shall have the rights set forth in **Appendix A** of the DIR Contract.

4.7 Accepted Deliverables – Plans

Upon acceptance by HHSC, any Deliverable that describes a plan or other action to be performed by Vendor becomes a contractual obligation of Vendor. No Deliverables may be changed by the Vendor after acceptance by HHSC unless the change is accepted in advance in writing by the HHSC Project Manager.

5. Project Changes

HHSC may request Vendor to perform additional services beyond the scope of this SOW or to remove services from the SOW scope by issuing a written change request ("Change Request") describing with

reasonable specificity the additional services to be performed or removed and any related deliverables. Within five (5) business days of receipt of a Change Request from HHSC, Vendor will submit to the HHSC Project Manager a Change Request plan ("**Change Request Plan**") to add or remove the services described in the Change Request. Vendor's Change Request Plan will specify impacts to the Project Schedule, impacts to the work plan, and Vendor's proposed additional or reduced cost, if any, associated with the Change Request. If requested by HHSC, Vendor will negotiate Vendor's proposed Change Request Plan with HHSC. A Change Request Plan does not become effective under the Contract until it is incorporated in an Amendment executed by the Parties.

6. Project Management

6.1 Project Schedule

Vendor will tightly and proactively manage Vendor's adherence to the Project Schedule throughout performance to ensure timely completion of this SOW, including by adding additional personnel, escalating issues within Vendor's organization as needed, communicating schedule, budget or scope risks to the HHSC Project Manager on a timely basis, and any other steps requested by the HHSC Project Manager to support timely completion of the Services. HHSC will not consider any revisions to the Project Schedule proposed by Vendor. Based upon the Project Schedule provided by the Vendor and accepted by HHSC, HHSC may set milestones for review to ensure the timely completion of the Contract.

6.2 Project Reporting and Tracking

Vendor will continuously monitor and track Vendor's progress toward completion of the SOW. Vendor shall meet the requirements of **Section 3.4** above, **Additional Project Deliverables**.

6.3 Communication and Meetings

Vendor will adhere to and fulfill the communication plan approved by HHSC during Phase I of the project. Unless approved otherwise by HHSC in writing in advance, all meetings are face-to-face and will be held at times and locations chosen by HHSC. HHSC will consider Vendor's preferences and will not unreasonably forbid teleconferencing. Vendor will include HHS System personnel, as requested or approved by the HHSC Project Manager, in meetings and work sessions. Attendance by Vendor personnel as specified in the communication plan (or Vendor's mutually agreed designees) is mandatory unless approved otherwise by HHSC in advance in writing. In the event of a designated Vendor personnel's sudden and unplanned unavailability to attend a scheduled meeting, Vendor will immediately advise HHSC's Project Manager and work with HHSC to reschedule affected meetings with minimal impact to the Project Schedule.

Other specific required meetings include:

a. Kickoff meeting:
    i. Review of project SOW;
    ii. Introduction of HHSC and Vendor project staff; and
    iii. Q&A / clarification as needed;
b. Major status reviews scheduled by HHSC based on need;
c. Deliverable walk-through meetings;
d. Final presentation; and
e. Project close-out meeting.

6.4 Presentations

Throughout the course of Vendor's performance of the SOW, at HHSC's request Vendor will present information regarding the progress of the SOW activities to a variety of audiences; e.g., leadership, sponsors, stakeholders, management, team, business, and technical, regarding Vendor's activities and outputs. Meeting dates and agendas will be selected by HHSC. Vendor will provide presentation materials to the HHSC Project Manager for review at least five (5) business days prior to the event.

6.5 Knowledge Transfer

Vendor will adhere to and fulfill the knowledge transfer plan approved by HHSC during Phase I of the project. Knowledge transfer activities may be appropriate at multiple points throughout the completion of the project phases. The response requirements below direct vendors to include a draft version of their proposed knowledge transfer plan with their response to this SOW.

6.6 Performance Measures and Associated Remedies

HHSC will monitor Vendor's performance under any Contract resulting from this SOW solicitation. Vendor will provide all Services and Deliverables in conformance with all Contract requirements, including all warranties set forth in the DIR Contract and in this SOW.

In addition to the specified Deliverables, all work and activities performed by Contractor hereunder will be reviewed by HHSC for conformance to Contract requirements. If HHSC identifies any deficiencies or nonconformities with Contract requirements with respect to Vendor's activities hereunder, HHSC may notify Vendor of the deficiency or non-conformity and Vendor will undertake diligent efforts to promptly correct the deficiency and/or non-conformity. The foregoing is in addition to any other remedies HHSC may have under the Contract or at law or equity with respect to a failure of Vendor to comply with the requirements of the Contract.

7. Invoices

Vendor may submit invoices on a monthly basis for completed and approved Deliverables accrued during the preceding calendar month as provided herein. Vendor may include in its invoice **90%** of the applicable net deliverable cost for Deliverables completed in accordance with the SOW requirements during the preceding calendar month. Upon Vendor's receipt of HHSC's written acknowledgment that Vendor has completed all Deliverables and other required activities with respect to a phase in accordance with the Project Schedule and all other requirements hereunder, Vendor may submit an invoice for the remaining **10%** of payable deliverable amounts for all Deliverables for the applicable project phase. Initial rejection of a Deliverable by HHSC does not disqualify Vendor from submitting an invoice for the remaining **10%** of payable deliverable amounts at the close of any project phase, ***provided that*** the rejected Deliverable is corrected, resubmitted, and approved by HHSC prior to the Deliverable due date provided in the Project Schedule. Payments will be made in accordance with **Appendix A** of the DIR Contract. Vendor must include in its response a draft version of the Vendor's proposed invoice template. Purchase Orders will be issued for each specific fiscal year and associated phases and Deliverables.

8. HHSC/Vendor-Furnished Equipment and Work Space

8.1 Restrictions on Access and Use

Vendor acknowledges and accepts that data and information that Vendor may have access to in the

course of performing the Services is subject to various federal and state laws, and that misuse of such data or information may result in civil and criminal enforcement actions and penalties. Subject to Vendor and Vendor's personnel executing, agreeing to, and complying with the applicable HHSC policies and agreements with respect to Vendor's access to and use of HHS System equipment, materials, data, and information, including without limitation **Exhibit C**, **HHS Information Security Acceptable Use Policy (AUP)**, **Exhibit D**, **Health and Human Services Acceptable Use Agreement (AUA)**, and **Exhibit E**, **HHS System Data Use Agreement**, and subject to successful completion by Vendor of **Exhibit E-1**, **HHS System Security and Privacy Inquiry**, and by Vendor's personnel of required background checks, HHSC will make the equipment, materials, data and information available to Vendor's personnel as described in this **Section 8**, solely for Vendor's use in performing the Services. Any approvals or access granted by HHSC as described by this **Section 8** may be revoked by HHSC at any time in HHSCs sole discretion upon notice to Vendor by HHSC.

8.2 HHSC Furnished Equipment and Work Space

Unless HHSC has approved otherwise in advance in writing, Vendor is only allowed to use HHSC-furnished equipment, including laptops, storage devices, and networks. No non-HHSC equipment or networks may be used for Vendor's performance hereunder, including but not limited to, personal computers and external storage devices. HHSC will supply Vendor's personnel badges for building entry and access to email and file sharing capabilities. Vendor will have access to HHSC source systems data, as well as available data models, data dictionaries and metadata. HHSC will provide up to four (4) cubicles for Vendor staff use. HHSC will provide from four (4) to ten (10) HHSC issued computers/laptops for Vendor staff use. All Vendor Work Product and Deliverables will be stored at all times on the HHSC infrastructure in the format and version approved by HHSC. Vendor is to propose the most efficient and effective location of staffing, onsite and remote.

8.3 Vendor Furnished Equipment and Work Space

HHSC in its sole discretion may approve Vendor to remotely perform Services using Vendor equipment, including processing files to prepare for conversion or migration in a Vendor-controlled environment. Notwithstanding any such approval by HHSC, Vendor shall at all times comply with the information security standards, policies, and other requirements as may be provided or communicated to Vendor by HHSC, including without limitation **Exhibits C, D, and E** of this SOW, and applicable state and federal laws.

9. Contractor Warranties

9.1 General

Contractor warrants, represents, and covenants that:

a. its personnel assigned to the Project have the requisite availability, competence, skill, and resources necessary to perform the Services in a timely, competent, and professional manner in accordance with the highest industry standards;

b. Contractor will at all times comply with applicable state and federal laws;

c. Contractor has full rights and authority to enter into and perform the Services according to this Contract;

d. Contractor will use adequate numbers of qualified individuals with suitable training, education, experience, and skill to perform the Services;

e. Contractor personnel performing the Services will use a level of care commensurate with the

best industry practices for safeguarding highly sensitive personal data with respect to all HHSC data they have access to in the course of performing the Services, and Contractor personnel will individually sign and abide by the applicable HHSC confidentiality, acceptable use, and information security agreements as may be requested by HHSC; and

f. the Services, the Deliverables, and any Contractor intellectual property or third-party intellectual property provided to HHSC under this SOW will not infringe any United States patent, copyright, trademark, trade secret, or other proprietary right of any third party or contain any viruses or other malicious code that will degrade or infect any Deliverables, product, service, or any other HHS System software or equipment.

9.2 Warranty Period

Contractor warrants, represents, and covenants that the Work, including all Services and Deliverables, will conform to all requirements and specifications of the Contract for a period of one hundred and twenty (120) days after their acceptance by HHSC (the "**Warranty Period**").

9.3 Warranty Obligations

If during the Warranty Period HHSC determines that the Services or any Deliverable do not conform to the foregoing warranty, and not withstanding any prior acceptance by HHSC of the affected Deliverable or Services, HHSC may provide written notice to Contractor of such non-conformity, and Contractor will reperform the Services and/or correct the non-conforming Deliverable within ten (10) business days of receipt of HHSC's notice at no cost to HHSC.

9.4 HHSC Right of Offset

HHSC may revoke its acceptance with respect to any Services or Deliverable that HHSC has identified to Contractor as non-conforming and offset payments due to Contractor by the amounts previously paid for the non-conforming Services or Deliverable. If HHSC exercises the right of invoice offset, Contractor may submit a new invoice with respect to the applicable Services or Deliverable after re-acceptance by HHSC.

10. Project Termination

10.1 For Convenience

Without prejudice to any other remedies, HHSC may terminate this Contract at any time without cause by giving written notice to Contractor. If HHSC terminates for convenience, its only obligation is to pay for Work or Deliverables it accepts before the effective date of termination or for Services performed, where HHSC retains the benefit after the effective date of termination.

10.2 Immediate Termination

Without prejudice to any other remedies, HHSC may terminate this Contract effective immediately upon written notice:

a. if Contractor breaches any obligation with respect to: i) confidentiality, privacy, and/or data security; ii) warranties; iii) ownership and use of the Parties' respective intellectual property; or iv) assignment;

b. if Contractor advises HHSC that the Project has become infeasible or that Contractor is unable or unwilling to perform the Services;

c. if Contractor attempts to renegotiate the scope of the Project and/or the terms and conditions of the SOW in a manner that, in the sole determination of HHSC, would prevent or diminish the attainment of the original purpose or objectives of the Project; or

d. if Contractor ceases to perform the Services for five (5) or more consecutive business days, and such cessation was not reflected in the Project Schedule.

10.3 Notice to Cure

If HHSC determines that Contractor has breached any of its obligations hereunder in a manner not covered by **Section 10.2**, above, HHSC may provide written notice to Contractor of such breach. Contractor will have ten (10) calendar days to cure such breach. If the specified breach is not cured within this period, HHSC may at its discretion i) extend the period to cure such breach, or ii) terminate the Contract with immediate effect.

10.4 Effect of Termination

Within ten (10) calendar days of the effective date of termination of this Contract, Contractor shall return to HHSC all HHSC materials, equipment, documentation, software, diagrams, schematics, layouts, information, access badges, and all other HHSC property unless otherwise instructed in writing by HHSC. Contractor shall deliver to HHSC, and HHSC may retain and use, in accordance with the terms of the Contract, any Work or Deliverables that HHSC has accepted and for which HHSC has paid Contractor. HHSC may, in its sole discretion, extend the Contract to allow for the performance by Contractor of turnover assistance services, and Contractor will provide all such turnover assistance services as requested by HHSC, providing that such assistance will not exceed one hundred and twenty (120) calendar days. Contractor shall not have any right to retain and will promptly deliver to HHSC any information, documents, programs, writings, designs, records, data, memoranda, tapes and disks containing software, computer source code listings, routines, file layouts, record layouts, systems design information, models, manuals, documentation, notes or copies thereof, in original format or media form that it obtained, directly or indirectly, from HHSC in connection with this Contract. Contractor's obligations with respect to **Section 9**, **Contractor Warranties**, this **Section 10.4**, **Section 11**, **Liability**, and any obligations with respect to confidentiality and non-disclosure, shall survive any termination or expiration of this Contract.

11. Liability

11.1 Acknowledged Direct Damages

The following shall be considered direct damages for purposes of this Contract, and neither Party shall assert that they are indirect, incidental, collateral, consequential or special damages, or lost profits to the extent they result directly from the breaching Party's failure to perform in accordance with this Agreement:

a. costs and expenses of restoring or reloading any lost, stolen, or damaged HHSC data or confidential information;

b. costs and expenses of implementing a work-around in respect of a failure to provide the Services or any part thereof;

c. costs and expenses of replacing lost, stolen, or damaged equipment and materials;

d. cover damages, including the costs and expenses incurred to procure the Services or corrected Services from an alternate source;

e. costs and expenses incurred to bring the Services in-house or to contract to obtain the Services from an alternate source;

f. straight time, overtime, or related expenses incurred by either Party in performing (a) through (e) above, including overhead allocations for employees, wages, and salaries of additional employees, travel expenses, overtime expenses, telecommunication charges, and similar charges;

g. fines, penalties, sanctions, interest or other monetary remedies incurred as a result of a failure to comply with applicable laws;

h. liquidated damages assessed against Contractor, if any;

i. costs and expenses of protecting and compensating the State and its constituents after a Breach (as defined in Exhibit E, Data Use Agreement), including but not limited to notifications, fines and penalties, establishing a call center, and thirty-six (36) months of credit monitoring for affected individuals; and

j. Contractor's obligation of indemnification set forth in this Contract, including without limitation Exhibit E, Data Use Agreement.

The absence of direct damages listed in this Section shall not be construed or interpreted as an agreement to exclude it as a direct damage under this Agreement.

11.2 Limitation of Liability

Notwithstanding any provision of this Contract or the DIR Contract to the contrary, Contractor shall be liable for the full amount of direct damages arising from: i) any breach of Contractor's obligations hereunder, or ii) the negligent acts and/or willful misconduct of Contractor's employees, agents, representatives, and subcontractors.

12. SOW Solicitation Additional Terms and Conditions

12.1 Exceptions to Terms

HHSC has the right to negotiate the terms and conditions of any resulting Contract, consistent with the DIR Contract. **HHSC does not invite exceptions to these SOW terms and conditions**. Responding Vendors are responsible for reviewing the terms and conditions of this SOW and all of its exhibits, attachments, and addenda (if any). Prospective Vendors are advised that a Vendor's proposed modifications to the terms and conditions of this SOW will be taken into consideration by HHSC in determining, in its sole discretion, the response that offers best value for the State. Prospective Vendors are also reminded that neither Vendor nor HHSC may negotiate or agree to terms and conditions that conflict with or weaken the terms and conditions of Vendor's DIR Contract.

12.2 SOW Cancellation and Partial Award or Non-Award

HHSC has the right to cancel this SOW Solicitation after issuance, to make a partial award, or to make no award if HHSC determines that such action is in the best interest of the State.

12.3 HHSC Right to Reject Proposals or Portions of Proposals

HHSC has the right to reject, in whole or in part, any and all Responses to this SOW.

12.4 Costs Incurred by Vendors

Issuance of this SOW in no way constitutes a commitment by HHSC to award a Contract or to pay any costs incurred by any vendor in the preparation of a Response to this SOW. HHSC is not liable for any costs incurred by any Vendor prior to issuance of or entering into a formal agreement, contract, or

purchase order. Costs of developing proposals, preparing for, traveling to, or participating in oral presentations and site visits, or any other similar expenses incurred by a Vendor are entirely the responsibility of the Vendor, and will not be reimbursed in any manner by the State.

12.5 Incomplete Responses

HHSC may reject without further consideration a proposal that does not include a complete, comprehensive, or total solution as requested by the SOW.

12.6 Property of HHSC

All copies of Responses to this SOW submitted by Vendors to HHSC become the property of HHSC after submission. Except as otherwise provided in this SOW or the resulting Contract, all products produced by a Respondent, including without limitations the proposal, all plans, designs, software, and other Contract Deliverables, become the sole property of HHSC after submission.

12.7 Copyright Restriction

HHSC has the right to refuse to consider any Vendor Response that bears a copyright marking on any of its materials.

12.8 Texas Public Information Act Applicable to Responses

HHSC reminds Vendors that HHSC is subject to the Texas Public Information Act (PIA or the Act), Texas Government Code, Chapter 552, including those provisions applicable to third-party information (including third-party, proprietary information) received by a state agency, and responses may be disclosed to the public upon request. Subject to the PIA, certain information may be protected from public release. Respondents who wish to protect portions of the Solicitation Response from public disclosure should familiarize themselves with this law. Vendor acknowledges and agrees that HHSC will comply with the Public Information Act with respect to all materials received from Vendor in the course of this SOW solicitation. Information pertaining to the Solicitation will be withheld or released only in accordance with the PIA. Vendor is advised to consult Vendor's legal counsel if Vendor has questions about the scope and procedures applicable to Vendor under the Texas Public Information Act. Amendments to the PIA passed during the 86th Legislative Session specifically make "contracting information" public information that must be disclosed in response to a public information request unless otherwise excepted by the Act. S.B. 943, Acts 2019, 86th Leg., R.S. (to be codified as Tex. Gov't Code §§ 552.03(7), 552.0222). Legislative bills are available on the Texas Legislature Online website: https://capitol.texas.gov/Home.aspx.

In addition, pursuant to Texas Government Code Section 2261.253(a), HHSC is required to post executed contracts and the associated solicitation documents on the agency website. Contract documents posted to the web may include the Solicitation Response of any Respondent receiving a Contract.

HHSC does not have authority to agree that any information submitted will not be subject to disclosure. Disclosure is governed by the PIA. Respondents are advised to consult with their legal counsel concerning disclosure issues resulting from this process and to take precautions to safeguard trade secrets and proprietary or otherwise confidential information. If it is necessary for Respondent to include proprietary or confidential information (which may include, but is not limited to, trade secrets or privileged information), Respondent must clearly mark in bold red letters the term "**CONFIDENTIAL**" using at least 14-point font, on that specific part or page of the submittal which Respondent believes to be confidential. All submittals and parts of submittals that are not marked confidential will be

automatically considered to be public information. Should trade secrets or proprietary or otherwise confidential information be included in the submitted electronic copy, the content should be marked in the same manner as the original as stated above. In addition, Respondent should mark the medium with the word "CONFIDENTIAL." If HHSC receives a public information request seeking information marked by Respondent as confidential, Respondent will receive notice of the request as required by the Texas Public Information Act.

If HHSC receives a public information request for submittals and parts of submittals that are not marked confidential, the information will be disclosed to the public as required by the Texas Public Information Act. Note that pricing is not generally considered confidential under the Texas Public Information Act. Merely making a blanket claim that the entire Solicitation Response is protected from disclosure because it contains any amount of proprietary or confidential information is not acceptable and may make the entire Solicitation Response subject to release under the PIA.

12.9 TEC Form 1295

Pursuant to Section 2252.908 of the Texas Government Code, a successful Vendor awarded a contract greater than $1 million dollars or awarded a Contract that would require the successful Respondent to register as a lobbyist under Texas Government Code Chapter 305 must complete Form 1295 Certificate of Interested Parties which is located on the Texas Ethics Commission's (TEC) public website. The responding Vendor must submit to HHSC a completed and signed form with the certificate of filing number and date with their Response. HHSC then acknowledges Form 1295 at the TEC website. Rules and filing instructions may be found on the TEC's public website and additional instructions will be given by HHSC to successful Respondents; https://www.ethics.state.tx.us/tec/1295-Info.htm

13. Response Submission Instructions

13.1 Number of Copies

Respondent must submit one electronic copy of the proposal, compatible with Microsoft Office 2013, via email to PCSBIDS@hhsc.state.tx.us with a copy to brad.westbrook@hhsc.state.tx.us.
HHSC will not accept proposals submitted by telephone and facsimile. Additionally, Respondents are required to deliver 8 (eight) paper copies of the proposal to:

Health and Human Services Commission
Procurement and Contracting Services Building
ATTN: Brad Westbrook
1100 W 49th. MC 2020
Austin, Texas 78756

13.2 Time and Place of Submission

Respondent must submit all copies of the proposal to HHSC's Procurement and Contracting Services (PCS) Division no later than **November 1, 2019** at 2:00 P.M., CST. All proposals will be date and time stamped when received by PCS. The clock in the PCS office is the official timepiece for determining compliance with the deadlines in this procurement. HHSC has the right to reject late submissions. It is the Respondent's responsibility to appropriately mark and deliver the proposal to HHSC by the specified date.

14. Response Organization and Content

14.1 Overview

Vendor's Response must consist of the following parts:

Part 1 – Required Acknowledgments
Part 2 – Qualifications and Background
Part 3 – Technical Proposal
Part 4 – Price Proposal

Vendor's Response must be:

- Clearly legible;
- Sequentially page-numbered and include Vendor's name and the SOW number at the top of each page;
- Organized in the sequence outlined below;
- Correctly identified with the SOW number and submittal deadline;
- Responsive to all SOW requirements;
- Typed on 8½ by 11" paper;
- In Arial or Times New Roman font, size 12 for normal text, no less than size 10 for tables, graphs and appendices; and

Vendors are requested not to exceed 100 total pages in their responses, excluding required forms, Exhibits and resumes. Responses may not include marketing materials or pamphlets or other materials or information not specifically requested in this SOW solicitation.

14.2 Part 1 – Required Acknowledgments

Vendor will include in Part 1:

a. Signed SOW and addenda, if any;
b. Signed **Exhibit A**, **Contract Affirmations and Solicitation Acceptance**;
c. Acknowledgment of schedule acceptance as described in **Section 3.2**;
d. Acknowledgement of acceptance of all terms and conditions of the SOW; and
e. Acknowledgement of agreement to comply with the confidentiality and non-disclosure requirements stated in this SOW.

Each of the foregoing must be signed by Vendor's authorized representative with full legal and corporate authority to bind Vendor to the terms and conditions of this SOW solicitation.

14.3 Part 2 – Qualifications and Background

Vendor will include the following information in Part 2 of Vendor's Response:

a. Corporate Overview
Vendor will describe Vendor's company background as it relates to projects similar in scope and complexity to the project described in this SOW. If Vendor's proposal includes the use of subcontractors, Respondent will include a similar description of each subcontractor's company background and experience. Vendor will also include Vendor's current organization chart and management team résumés. Vendor will disclose any party other than Vendor that owns a controlling interest in Vendor, or that has the corporate right or authority to direct the actions of Vendor, and HHSC has the right to require

such controlling party to unconditionally guarantee performance by Vendor in each and every term, covenant, representation, and warranty of the Contract as a condition to HHSC entering into any Contract with Vendor. Vendor is to have explicit PPM experience and expertise in implementing and configuring PPM platform, including but not limited to Partner Program or the Software Partner Program.

b. Staff Capabilities

Vendor will identify and describe Vendor's and its subcontractor's (if any) proposed labor skill set and provide résumés of all proposed key personnel (as defined by Vendor). These key personnel cannot be changed or removed without the permission of HHSC except for cause or other disciplinary reason. Vendor will provide HHSC the opportunity to interview and approve proposed replacement staff for the key personnel positions on Vendor's project team. Résumés must demonstrate experience from the last five (5) years that is germane to the position proposed. Résumés should include work on projects cited under the Respondent's company experience, and the specific functions performed on such projects. Each résumé should include at least three (3) references from recent projects. References may not be the Respondent's or subcontractor's employees. Vendor should reflect any relevant certifications for their staff.

c. Staff Organization

Vendors will provide a project organization chart, with proposed prime and subcontractor staff assigned to this project. In addition, Vendor will provide a high-level narrative description of the project team organization, teams and roles. Vendor's personnel proposed for the project must be available for interviews during the selection process.

d. Service Capabilities

Vendor shall provide evidence of its services capabilities, including, but not limited to:

i. description of three (3) projects of similar size and scope that Vendor has conducted within the past five (5) years;
ii. description of experience providing similar Deliverables in public sector, specifically state and local government;
iii. an outline of its capability to deliver the required services, including process, functional and technical expertise; and
iv. Vendor may also include the types of information that it anticipates providing as part of each Deliverable.

e. References

Using **Exhibit F**, **Experience Reference Form**, Vendor must supply at least three (3) references that verify Vendor has successfully performed the required services within the last five (5) years for a paying customer external to Vendor's organization and that customer has successfully implemented those recommendation(s). Note: HHSC will contact these references to validate. For each provided reference, Vendor must provide a completed and signed release of liability form, found at **Exhibit F-1**, **Respondent Release of Liability.**

In addition to the references required above, if Vendor will be using subcontractors to perform the Services, Vendor must use the forms referenced above to supply at least two (2) references that verify Vendor's proposed subcontractors have successfully performed the required services within the last five (5) years for a paying customer external to Subcontractor's and Vendor's organizations.

f. Financial Capacity

Vendors are not required to submit evidence of financial capacity with their proposals. However, HHSC has the right to request such information at a later date, including during any Contract, and Vendor will

provide such information as requested. HHSC has the right to require Vendor to procure one or more performance, fidelity, payment or other bonds, if during the term of the Contract; HHSC in its sole discretion determines that there is a business need for such requirement.

14.4 Part 3 – Technical Proposal

Vendor will include the following information in Part 3 of Vendor's Response:

a. Project Schedule
Vendor will provide a proposed Project Schedule that includes Deliverable Due Dates for each Deliverable identified in **Section 3.3** of this SOW. Vendor's proposed Project Schedule will provide reasonable interims between the timing of Deliverables: i) to provide HHSC with adequate visibility into activity progress, and ii) to allow the required Deliverable walk-through, review and correction process described in **Section 4** of this SOW. Multiple Deliverables can be delivered in a Deliverable walk-through meeting. Vendor is reminded that the final ten percent (**10%)** retainage payment at the close of every project phase is dependent, among other things, on Vendor's timely completion of each Deliverable in the associated phase in accordance with the Project Schedule. Vendors are urged to take these dependencies and review cycles into consideration in developing the proposed Project Schedule.

b. Project Work Plan
Vendor's response will include a project work plan that describes Vendor's proposed processes and methodologies for providing all components of the Scope of Work described in **Sections 2 and 3** of this SOW. Vendor's project work plan will address the Deliverables specified in **Section 3.3** of this SOW, and shall include:

i. A description of key activities and milestones;
ii. A detailed methodology description of Vendor's approach to analyze, assess, validate, document and complete each sprint/iteration;
iii. A description of the resources necessary from HHSC to support the process, including estimates of time needed from HHSC's subject matter experts and high-level analysis of data gathering requirements; and
iv. Any assumptions and/or dependencies of the project.

c. Sample Requirements Traceability Matrix

d. Sample Weekly Status Report

e. Sample Issue Log

f. Sample Risk Log

g. Sample Communication Plan

h. Draft Knowledge Transfer Plan

i. Value-added Benefits

Vendor will include in its Response a description of any services or deliverables that are not required by the SOW that Vendor proposes to provide at no additional cost to HHSC. Vendors are not required to propose value-added benefits, but inclusion of such benefits may result in a more favorable evaluation by HHSC.

14.5 Part 4 – Price Proposal

Vendor will include the following information in Part 4 of Vendor's Response:

a. Vendor Price Sheet

Vendor's sole compensation, and HHSC's sole obligation for payment to Vendor for performing the Services (including all Work Product delivered to HHSC), is the Deliverables-associated payments described herein. Vendor must complete **Exhibit G**, **Vendor Price Sheet**, and include Vendor's Price Sheet with Vendor's Response as a separate file or document. Vendor is reminded to take into consideration the ten percent (**10%**) retainage provided in **Section 7** of this SOW when developing its price sheet.

b. Vendor Form of Invoice

Vendor must also include in Part 4 a draft version of Vendor's proposed invoice template. Invoices shall include at a minimum the HHSC SOW contract number, Deliverable number, date of Deliverable acceptance by HHSC, Deliverable price (from Vendor Price Sheet), and the amount charged for the Deliverable, reflecting the ten percent (**10%)** retainage described in **Section 7** of this SOW.

14.6 Exceptions to Terms and Conditions

HHSC does not invite exceptions to the terms and conditions of this SOW. Any responding Vendor that includes in its response exceptions to the terms and conditions of this SOW may be automatically disqualified by HHSC, in HHSC's sole discretion.

15. Historically Underutilized Business Participation

Because this solicitation is released under the jurisdiction of the DIR co-operative contracts program, Respondents are not required to submit a **HUB subcontracting plan** (HSP) with their proposal at the time of submission. Any Contract resulting from this SOW will incorporate the awarded Contractor's DIR HSP as part of that Contract. If subcontractors are used in the delivery of the goods and/or services, the awarded Contractor is required to submit monthly progress reports, in the prescribed format, to HHSC's HUB Program Office. When applicable, the reports must include a narrative description of the Contractor's good-faith efforts and accomplishments, and financial information reflecting payments to all subcontractors, including HUBs. **All Respondents must certify in their proposal that their DIR HSP is up to date and accurate.**

16. Proposal Evaluation

16.1 Conformance with State Law

HHSC will evaluate SOW Responses in accordance with Title 10, Subtitle D of the Texas Government Code. HHSC shall not be obligated to accept the lowest priced SOW response, but, may make an award to the Vendor that provides the best value to the State. HHSC will consider capabilities or advantages that are clearly described in the Responses, which HHSC may require to be confirmed by oral presentations, site visits, demonstrations, and references contacted by HHSC. HHSC has the right to contact individuals, entities, or organizations that have had dealings with Vendor or proposed staff, whether or not identified in the Vendor's Response.

16.2 Initial Compliance Screening

HHSC will perform an initial administrative screening of all SOW Responses received. Unsigned SOW Responses, and SOW Responses that do not include all required forms and information may be subject to rejection by HHSC in its sole discretion without further evaluation. HHSC has the right to waive minor informalities in a Response and award contracts that are in the best interest of the State.

16.3 Specific Criteria

HHSC will evaluate Responses based on the following best value criteria, listed in order of precedence, with the relative weightings noted:

Technical Proposal and Approach to Project	**40%**
Price Proposal	**35%**
Strength of the Respondent Qualifications and Background	**20%**
Exceptions to Terms and Conditions	**5%**

16.4 Questions or Requests for Clarification by HHSC

HHSC reserves the right to ask questions or request clarification from any Respondent at any time during the SOW procurement process, including during oral presentations, site visits, or during the best and final offer (BAFO) process.

16.5 Oral Presentations and Site Visits

HHSC reserves the right to require an oral presentation from any or all responding Vendors to make a determination for award recommendation. Oral presentations will be evaluated using the evaluation tool criteria. Information from the oral presentation will be used in addition to the scoring of the previous criteria listed above. Respondents will be provided with advance notice of any such oral presentation and are responsible for their own presentation equipment. Advance notice will include an agenda for the oral presentation specifying the areas expected to be elaborated or presented by the Respondent in its presentation. Failure to participate in the requested presentation may eliminate a Vendor, in HHSC's sole discretion, from further consideration. HHSC is not responsible for any costs incurred by Vendors in preparation for or delivery of any oral presentation.

HHSC may require site visits from any or all responding Vendors. HHSC will notify selected Vendors of the time and location of site visits. Failure to permit or participate in the requested site visit may eliminate a vendor, in HHSC's sole discretion, from further consideration. HHSC is not responsible for any costs incurred by Vendors in preparation for or conducting any site visit.

16.6 Best and Final Offers

HHSC may, but is not required to, permit responding Vendors who have not been otherwise disqualified or eliminated to prepare one or more revised offers. For this reason, responding Vendors are encouraged to treat their original proposals, and any revised offers requested by HHSC, as best and final offers (BAFO). If BAFOs are requested by HHSC and submitted by the Respondent, they will be evaluated (using the stated BAFO criteria), scored, and ranked by the evaluation committee. The BAFO criteria is the evaluation tool criteria considered for the solicitation. HHSC reserves the right to conduct more than one BAFO. The award will then be granted to the highest scoring Respondent. However, a Respondent should provide its best

offer in its original proposal. Respondents should not expect or assume that HHSC will request a BAFO.

16.7 Discussions with Responding Vendors

HHSC may, but is not required to, conduct discussions with all, some, or none of the responding Vendors, for the purpose of obtaining the best value for HHSC under any Contract. HHSC may conduct discussions with responding Vendors for the purpose of:

- Obtaining clarification of proposal ambiguities;
- Requesting modifications to a proposal; and/or
- Obtaining a best and final offer.

HHSC may make an award prior to the completion of discussions with all responding Vendors if HHSC determines that the award represents best value to the State.

16.8 Award

HHSC intends to award one contract, if any, for all project phases of this SOW. HHSC has the right to award some, all, or none of this SOW.

17. Additional Terms and Conditions

Vendor is representing itself to HHSC as an industry expert in the subject matter of this SOW with the expertise and resources necessary for successful and timely completion of the SOW.

17.1 External Factors

Certain external factors outside the control of HHSC may materially affect the feasibility of the project undertaken with this SOW, including without limitation budgetary and resource constraints, approvals required from state and/or federal entities outside of HHSC, and changes to laws governing HHSC (collectively, "**External Factors**"). If HHSC determines that sufficient funds are not available to support the project or that any other External Factor has rendered the project infeasible, HHSC will have the right to withdraw the SOW or terminate the Contract without penalty.

17.2 Standards of Conduct

In accordance with Title 1 Texas Administrative Code (TAC), Part 15, Sec. 391.505(a), the Contractor and its subcontractors must implement standards of conduct for their own personnel and agents on terms at least as restrictive as those applicable to HHSC contracting personnel. These standards of conduct must adhere to the ethics requirements adopted in 1 TAC, Part 15, Sec. 391.505(a), in addition to any ethics policy, or code of ethics approved by the Executive Commissioner of HHSC.

17.3 U.S Department of Homeland Security's E-Verify System

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

1. All persons employed to perform duties within Texas, during the term of the Contract; and
2. All persons (including subcontractors) assigned by the Contractor to perform work pursuant to the Contract, within the United States of America.

The Contractor shall provide, upon request of HHSC, an electronic or hardcopy screenshot of the confirmation or tentative non-confirmation screen containing the E-Verify case verification number for attachment to the Form I-9 for the three most recent hires that match the criteria above, by the Contractor, and Contractor's subcontractors, as proof that this provision is being followed. **If this certification is falsely made, the Contract may be immediately terminated by HHSC, at the discretion of the State and at no fault to the State, with no prior notification. The Contractor shall also be responsible for the costs of any re-solicitation that the State must undertake to replace the terminated Contract.**

17.4 Vendor Due Diligence

HHSC advises and puts Vendor on notice that the documentation, artifacts, diagrams, and other written information to be provided to Vendor by HHSC to describe HHS's current environment may be outdated, incomplete, inaccurate, and otherwise deficient. HHSC is specifically engaging Vendor for Vendor's expertise in identifying and correcting such inaccuracies and deficiencies and providing HHSC a complete, thorough, and accurate view and assessment of the relevant HHS System environments, systems, and data analytics and reporting needs and recommended strategies. Vendor shall exercise Vendor's due diligence in reviewing and analyzing all documentation provided by HHSC to identify and detect the flaws and inaccuracies in the HHS System documentation and not duplicate or otherwise incorporate those documentation errors into Deliverables. HHSC will make HHSC IT staff available to Vendor by request through the HHSC project contact for this engagement. Vendor is encouraged to interview HHSC IT staff and request whatever additional documentation Vendor requires to satisfy Vendor that it has a correct understanding of the current HHS System environment. If at any time Vendor determines that it is unable to obtain the information from HHSC that Vendor requires in order to produce true, correct, and complete Deliverables, Vendor will immediately so notify the HHSC project contact.

17.5 Entire Agreement

This SOW and the DIR Contract contain all the terms and provisions between HHSC and Vendor relating to the matter set forth herein and no prior or contemporaneous agreement or understanding pertaining to the same, including, without limitation, any electronic mail correspondence between the parties involved or other correspondence, shall be deemed or considered included in this SOW. No modification, addendum to or amendment of this SOW shall be effective unless set forth in writing and executed by the duly authorized representatives of HHSC, DIR, and Vendor.

SIGNATURE PAGE:

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

Legal Name of Vendor: _____

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 A. AFFIRMATIONS AND SOLICITATION ACCEPTANCE

In this document, the terms Respondent, Contractor, Applicant, and Vendor, when referring to the following affirmations (whether framed as certifications, representations, warranties, or in other terms) refer to Respondent, and the affirmations apply to all Respondents regardless of their business form (e.g., individual, partnership, corporation).

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 represents and warrants that it will comply with the requirements of Section 552.372(a) of the Texas Government Code. Except as provided by Section 552.374(c) of the Texas Government Code, the requirements of Subchapter J (Additional Provisions Related to Contracting Information), Chapter 552 of the Government Code, may apply to the contract and the Respondent agrees that the contract can be terminated if the Respondent knowingly or intentionally fails to comply with a requirement of that subchapter.
5. 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.
6. Respondent's Solicitation Response will remain a firm and binding offer for 240 days from the date the Solicitation Response is due.

7. Respondent shall not assign its rights under the contract or delegate the performance of its duties under the contract without prior written approval from HHSC. Any attempted assignment in violation of this provision is void and without effect.

8. Respondent accepts the Solicitation terms and conditions unless specifically noted by exceptions advanced in the form and manner directed in the Solicitation. No exceptions, terms, or conditions will be considered if not advanced in the form and manner directed in the Solicitation. Respondent agrees that all exceptions to the Solicitation as well as terms and conditions advanced by Respondent that differ in any manner from HHSC's terms and conditions are rejected unless expressly accepted by HHSC in writing in a fully executed contract.

9. 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.

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

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

12. 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.

13. 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):

    - □ Goods produced or offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
    - □ Goods produced in Texas or offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
    - □ Agricultural products grown in Texas
    - □ Agricultural products offered by a Texas bidder
    - □ Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
    - □ Services offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
    - □ Texas Vegetation Native to the Region
    - □ USA-produced supplies, materials or equipment
    - □ Products of persons with mental or physical disabilities
    - □ Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel
    - □ Energy efficient products
    - □ Rubberized asphalt paving material
    - □ Recycled motor oil and lubricants
    - □ Products produced at facilities located on formerly contaminated property

- □ Products and services from economically depressed or blighted areas
- □ Vendors that meet or exceed air quality standards
- □ Recycled or reused computer equipment of other manufacturers
- □ Foods of higher nutritional value
- □ Commercial production company or advertising agency located in Texas

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. Respondent certifies that it is not listed in the prohibited vendors list authorized by Executive Order 13224, *"Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism,"* published by the United States Department of the Treasury, Office of Foreign Assets Control.

20. 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.

21. 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.

22. Under Section 2155.0061 of the Texas Government Code, the 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.

23. 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.

24. 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.

25. 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).

26. 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.

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

28. 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:

- providing equivalent access for effective use by both visual and non-visual means;
- presenting information, including prompts used for interactive communications, in formats intended for non-visual use; and
- 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.

29. 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.

30. 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.

31. Respondent represents and warrants that it will comply with the requirements of Section 2054.5192 of the Texas Government Code relating to cybersecurity training and required verification of completion of the training program.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. If this Solicitation is for an employment contract, a professional services contract under Chapter 2254 of the Texas Government Code, or a consulting services contract under Chapter 2254 of the Texas Government Code, Respondent represents and warrants that neither Respondent nor any of Respondent's employees including, but not limited to, those authorized to provide services under the contract, were former employees of an HHS Agency during the twelve (12) month period immediately prior to the date of the execution of the contract.

39. If this Solicitation is for consulting services,

(A). In accordance with Section 2254.033 of the Texas Government Code, a Respondent offering to provide consulting services in response to this solicitation who has been employed by, or employs an individual who has been employed by, HHSC or another State of Texas agency at any time during the two years preceding the submission of Respondent's Solicitation Response must disclose the following information in its Solicitation Response and hereby certifies that this information is true, correct, and complete:

(1) Name of individual(s) (Respondent or employee(s)): _____

(2) Status (circle one): Respondent Employee

(3) The nature of the previous employment with HHSC or the other State of Texas agency:

_____

(4) The date the employment was terminated and the reason for the termination:

_____

(5) The annual rate of compensation for the employment at the time of its termination: _____

If more than one individual is identified in A(1) above, Respondent must provide responses to A(2)-(5) as to each identified individual. To satisfy this requirement, Respondent must attach a separate page or pages, as necessary, and include the information required in Section A, including subsections (1)-(5). Respondent must identify here how many pages, if any, are attached: _____. Respondent acknowledges, agrees, and certifies that all information provided is true, correct, and complete on this and all attached pages.

(B). If no information is provided in response to Section A above, Respondent certifies that neither Respondent nor any individual employed by Respondent was employed by HHSC or any other State of Texas agency at any time during the two years preceding the submission of Respondent's Solicitation Response.

40. Pursuant to Section 2271.002 of the Texas Government Code, Respondent certifies that either (i) it meets an exemption criteria under Section 2271.002; or (ii) it does not boycott Israel and will not boycott Israel during the term of the contract resulting from this Solicitation. If Respondent refuses to make that certification, Respondent shall state here any facts that make it exempt from the boycott certification:

_____
_____
_____.

41. Respondent understands, acknowledges, and agrees that, pursuant to Article IX, Section 6.25 of the General Appropriations Act (the Act), to the extent allowed by federal and state law, money appropriated by the Texas Legislature may not be distributed to any individual or entity that, during the period for which funds are appropriated under the Act: (i) performs an abortion procedure that is not reimbursable under the state's Medicaid program; (ii) is commonly owned, managed, or controlled by an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program; or (iii) is a franchise or affiliate of an entity that performs an abortion procedure that is not reimbursable under the state's Medicaid program. The provision does not apply to a hospital licensed under Chapter 241, Health and Safety Code, or an office exempt under Section 245.004(2), Health and Safety Code. Respondent represents and warrants that it is not ineligible, nor will it be ineligible during the term of the contract resulting from this Solicitation, to receive appropriated funding pursuant to Article IX, Section 6.25.

42. Respondent understands, acknowledges, and agrees that, pursuant to Chapter 2272 of the Texas Government Code, except as exempted under that Chapter, HHSC cannot contract with an abortion provider or an affiliate of an abortion provider. Respondent certifies that it is not ineligible to contract with HHSC under the terms of Chapter 2272 of the Texas Government Code. If Respondent refuses to make that certification, Respondent shall state here any facts that make it exempt from the certification:

_____
_____
_____.

43. 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.

44. 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.

45. 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.

46. 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 B: SOW SIGNATURE DOCUMENT FOR
TEXAS HEALTH AND HUMAN SERVICES COMMISSION CONTRACT NO. HHS[xxxxxxxxx],
A STATEMENT OF WORK UNDER
DIR CONTRACT #DIR-TSO-[xxxx]

I. PURPOSE

This is a contract (the "**Contract**") by and between the Texas Health and Human Services Commission ("**HHSC**" or "**System Agency**"), an administrative agency within the executive department of the State of Texas and having its principal office in Austin, TX, and [XXXXXXX] ("**Vendor,**" "**Contractor**," or "**Respondent**"), a [state] [type of entity] having its principal office at [physical address] (each a "**Party**" and collectively the "**Parties**"). Upon execution by the Parties, the additional contract documents listed below (collectively, the "**Statement of Work**" (SOW)) shall be incorporated in their entirety into this SOW Signature Document. The Parties execute this Contract as a procurement by System Agency under and via DIR Contract # DIR-TSO-[xxxx] (the "**DIR Contract**"), and they agree that the terms of the DIR Contract apply to and govern this Contract as described herein. Capitalized terms used herein shall have the meanings provided in the Statement of Work or the DIR Contract unless defined herein.

II. LEGAL AUTHORITY

This Contract is authorized by and in compliance with the provisions of Title 10, Subtitle D of the Texas Government Code, including Chapters 2155 and 2157, and Chapter 531 of the Texas Government Code.

III. SERVICES TO BE PROVIDED

Contractor shall perform the Services in accordance with the terms and conditions of this Contract and the terms and conditions of the DIR Contract. The Statement of Work includes the documents listed below, each of which is attached hereto and incorporated herein by reference. In the event of a conflict between the terms and conditions set forth in the documents that make up this Contract, the controlling document shall be this Signature Document, then **Attachment A**, then **Attachment B**, then **Attachment C**, then **Attachment D**[.][, then **Attachment E**]. 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 SOW Signature

Document and terminates upon the earlier of completion of the Project or [Month spelled out DD, YYYY], whichever occurs first, unless renewed, extended, or terminated pursuant to the terms and conditions of the Contract. System Agency, at its sole discretion, may extend the Contract beyond [Month spelled out DD, YYYY] as necessary up to a maximum of twenty-four (24) months to address immediate operational or service delivery needsas determined by System Agency.

V. BUDGET

The total amount payable to Contractor under this Contract will not exceed **[TOTAL CONTRACT AMOUNT ($00.00)]**.

VI. CONTRACT REPRESENTATIVES

The following will act as the representative (the "**Project Manager**") authorized to administer activities under this Contract on behalf of their respective Party.

4. System Agency

[Agency Name]
[Address]
Austin, TX 78756
Attention: [Project Manager]

5. Contractor

[Vendor Name]
[Address 1]
[Address 2]
Attention: [Project Manager]

VII. LEGAL NOTICES

Any legal notice required under this Contract shall be provided as directed in the DIR Contract, provided also that an additional copy shall be provided to System Agency as follows:

Texas Health and Human Services
Commission Attn: Office of the Chief
Counsel
4900 N Lamar Blvd.; MC 1100
Austin, TX 78751

Legal notice given by Contractor to System Agency shall be deemed effective when received by System Agency. Any Party may change its address for notice by written notice to the other Parties.

VIII. ENTIRE AGREEMENT

This Contract and the DIR Contract contain all the terms and provisions between System Agency

and Contractor relating to the matter set forth herein and no prior or contemporaneous agreement or understanding pertaining to the same, including, without limitation, any electronic mail correspondence between the parties involved or other correspondence, shall be deemed or considered included in this agreement. No modification, addendum to or amendment of this Contract shall be effective unless set forth in writing and executed by the duly authorized representatives of System Agency and Contractor. Contractor represents and warrants that the individual signing below on Contractor's behalf has full corporate authority to legally bind Contractor to the terms and conditions of this Contract. These representations and warranties are made for the purpose of inducing the State to enter into this contract.

- **This SOW is not valid without DIR signature. This SOW may be modified at any time provided such changes are agreed to by both parties, are in writing, and are signed by both parties and DIR.**

SIGNATURE PAGE FOLLOWS

SIGNATURE PAGE FOR HHSC STATEMENT OF WORK CONTRACT NO. HHS[xxxxxxxxx] UNDER DIR CONTRACT # DIR-TSO-[xxxx]

HEALTH AND HUMAN SERVICES COMMISSION:	[Vendor Name]:
_____	_____
[Name]	Name: [xxxxxxxxxx]
[Title]	Title: [xxxxxxxxxxxx]
Date:_____	Date: _____

The DIR signature below is solely to verify that the scope of work is within the scope of the DIR contract being utilized. The DIR signature does not make DIR a party to the SOW Signature Document or to any constituent document.

DIR REVIEW – HHSC SOW ID # HHS[xxxxxx]

_____

Hershel Becker

Chief Procurement Officer

Date: _____

THE FOLLOWING ATTACHMENTS TO THIS SOW SIGNATURE DOCUMENT ARE HEREBY ATTACHED AND INCORPORATED BY REFERENCE:

Attachment A: HHSC Statement of Work, including all exhibits
Attachment B: HHSC Uniform Terms and Conditions – Vendor
[Attachment B-1: HHSC Special Conditions – Vendor]
Attachment C: HHSC Data Use Agreement ver. 8.5
Attachment C-1: HHSC Security and Privacy Initial Inquiry
Attachment D: Contractor's Price Quote
[Attachment E: Contractor's Response]

Exhibit C: HHS Information Security Acceptable Use Policy (HHS AUP):

HHS Information Security Acceptable Use Policy (HHS AUP)

Version 1

Revised

September 25, 2015

Purpose

The purpose of this document is to inform Users of their responsibilities concerning the use and protection of HHS Information Resources (IR) which includes HHS data, information systems, software, and equipment. The term "User" is used in the document to refer specifically to an HHS IR User that is authorized access to HHS Information Resources. The HHS Information Security Acceptable Use Policy (HHS AUP) works in conjunction with the *HHS Information Security Policy (IS-Policy)* and *HHS Acceptable Use Agreement (AUA)*.

All HHS (IR), which have not been specifically identified as the property of other parties, will be treated as an HHS asset. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of these resources is prohibited. All User activity on HHS IR is subject to logging and review.

Every information resource privilege that has not been explicitly authorized is prohibited. Such privileges will not be authorized for any HHS business purpose until approved by the Information Owner, or designee, in writing or by electronic acknowledgement. Agency Information Owners are responsible to approve, justify, document, and be accountable for exceptions to the security requirements in this document. Information entrusted to HHS will be protected in a manner consistent with its data classification and in accordance with all applicable standards, controls, agreements, and laws.

Users formally acknowledge their understanding, acceptance, and compliance with the HHS Information Security Acceptable Use Policy (IS-AUP) when signing the *HHS Acceptable Use Agreement (AUA)*. Users are further informed of their responsibilities when taking the annual *HHS Information Security Acceptable Use Training*

Scope

This policy applies to all HHS Workforce Members (employee, trainee, intern, and volunteer or staff augmentation contractor) and Users of HHS information resources. Any person or entity granted access to HHS IR, and representatives of other agencies of state government must comply with the standards set forth in this document. This policy excludes HHS clients, who receive services from HHS. Clients are not considered Users and therefore are not in scope.

Use of HHS Information Resources

- The User of an HHS Information Resource has the responsibility to:
  - use the resource only for the purpose specified by HHS or the Information Owner;
  - comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
  - formally acknowledge compliance with security policies and procedures by signing the HHS Information Resource Acceptable Use Agreement.
- Security incidents shall be immediately reported to the user's supervisor/manager, the agency Information Security Officer and other agency or HHS offices as applicable, as further defined in the HHS Incident Response Plan.
- HHS establishes the policies for verifying the identity of a User, process, or device, as a prerequisite for granting access to resources in an information system.
- Information Resources are intended to be used in support of official state-approved business.
- Limited personal use of IR may be allowed and is described in other policies and procedures of the HHS Agency by which users are granted access.

- Proper authorization for all users is required for access to all information owned by HHS Agencies, except for information that is maintained for public access.
  Users will not attempt to access or alter any HHS information without authorization and in the performance of their job duties.
- Users will not enter any unauthorized information, make any unauthorized changes to information, or disclose any information without proper authorization. Unauthorized access to an HHS Information Resource, allowing another party unauthorized access to, or maliciously causing a computer malfunction are violations under Chapter 33 of the Texas Penal Code ("Computer Crime Law") and are punishable by fines, incarceration, or both.
- Users must not intentionally access, create, store, or transmit any material that may be offensive, indecent, or obscene unless required as part of their job duties.
- Users may not engage in any activity that is harassing, threatening, abusive, degrades the performance of IR, deprives or reduces an authorized User's access to resources, or otherwise circumvents any security measure or policy.
- Users shall not use any HHS IR to gain personal benefit.
- Any User who becomes aware of or suspects an actual or possible computer security incident, weakness, misuse or violation of any policy related to the security and protection of those resources must immediately report such to their supervisor/manager, their agency Information Security Officer (ISO) and other agency or HHS offices as applicable, as further defined in the HHS Incident Response Plan.
- Users shall not use HHS IR for purposes of political lobbying or campaigning.
- Users shall not violate copyright laws by inappropriately distributing protected works.
- Users shall not pose as anyone other than oneself, except when authorized to send messages for another when serving in an administrative support role.

System Access

- Users will be given access only to those systems to which they require access in the performance of official duties.
- Users will not enter any unauthorized data, make any unauthorized changes to data, or disclose any data without proper authorization.
- Users must sign or electronically acknowledge the *HHS Acceptable Use Agreement (AUA)* stating they have read and agree to follow HHS requirements regarding computer security policies and procedures before access is given to any IR. Additional documentation or training may also be required. As an example, Users with access to Federal Tax Information must take *Safeguarding Internal Revenue Service Federal Tax Information* training annually.
- At a minimum new Users must complete the HHS *Information Security Acceptable Use Training* prior to, or within thirty days of, being granted access to any HHS IR.
- Users must reaffirm their commitment to the protection of HHS IR by completing the HHS *Information Security Acceptable Use Training* on an annual basis.

User Credentials

- Users will receive and be required to use credentials (User ID and Password) to gain access to and to use HHS Information Resources.
- Users will create and use a strong password with a minimum of eight characters in length containing upper case alpha, lower case alpha, numerical, and special characters. (It is noted further requirements for passwords may be issued.)
- Users will not construct a password from obvious user names or passwords, such as personal information (i.e. telephone numbers, relative's names, pet's names, or passwords used for personal business, etc.). Passwords

should be memorized and never be written down or stored unencrypted. Users will not reveal their personal password to anyone, including administrative assistants or management.,

- Users will be held responsible for any violations of applicable law or agency policy related to HHS Confidential Information, HHS Agency sensitive information, or HHS Information Resources, caused by acts or omissions, or for any harm, loss, or adverse consequences arising from the use of credentials, including any unauthorized use by a third party or contractor if such party gains access to credentials due to negligence or misconduct. Disciplinary actions up to and including dismissal and civil or criminal prosecution may result from any violations or misuse.
- Transactions initiated under a User's credentials will be considered as having been authorized and electronically signed by the User.
- Users will not use the same password for HHS accounts as for other non-HHS accounts (e.g., personal banking or other personal or business websites, etc.).
- Users will not use the "Remember Password" feature of applications, auto logon, embedded scripts or hard coded passwords outside of approved IT managed systems such as the Enterprise Portal or Enterprise Single Sign On (ESSO).
- If an account or password is suspected to have been compromised, report the incident to the Help Desk and change all passwords.
- Avoid others watching you type your password (shoulder surfing).
- Temporary passwords must be changed upon User's receipt of the password.

Software

- Users will use only agency approved and properly licensed software on HHS Information Resources. Any use of software on HHS Agency IR shall be in accordance with the applicable software license agreement.
- Users will not download or operate a peer-to-peer (P2P) file sharing system to transfer files (including music or video files).
- Users will not install or use any software on HHS Information Resources unless the software has been approved for use in accordance with HHS Agency policies and procedures[1].
- Users will not download, install or run application programs or utilities that reveal or exploit weaknesses in the security of a system without approval as part of the official systems security management process.
- Users will not use unapproved tools such as password cracking programs, packet sniffers, network-mapping tools, or port scanners without approval as part of the official systems security management process.
- Unauthorized use of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which HHS, the agency, or the User does not have an active license is strictly prohibited.
- Users will not disable or bypass malware protection software without the approval and involvement of appropriate HHS IT staff.

Network

- Users must not extend or re-transmit network capabilities without approval of the agency Information Resource Manager (IRM).
- Users must not install hardware, software, or any device (for example Bluetooth) that provides network services without the approval of the agency IRM.
  All HHS devices with wireless capability must be encrypted.
  Any wireless data transmissions that may contain agency sensitive or confidential information, including electronic Protected Health Information, must be encrypted.

[1] Agency Approved Software can be found at http://hhsc-online.hhsc.state.tx.us/handbook/software.html

- The use of wireless access points must meet authentication and encryption requirements set out in HHS security policy, standards, and controls.
- Users are prohibited from using or installing any device which functions in wireless mode in order to access data, transfer data or connect in any manner to HHS internal networks or systems without the approval of the Agency IRM, the CIO if no agency IRM exists, or a designee, and assistance of the Agency IT staff charged with this responsibility in their official job capacity.
- A system may not be connected to the HHS network until it is in a secure state and the network connection is reviewed and approved by the appropriate agency IRM or the CIO if no agency IRM exists.

E-mail

- Users should not open e-mail attachments or click on links within e-mails received from unknown senders, which may contain viruses or malware.
- Users will not send e-mail that violates HHS Agency policy, such as e-mail containing malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or inappropriate racist, gender, sexual, or religious content over state government e-mail.
- Confidential information shall be encrypted with an agency approved encryption technology. It is recommended that agency sensitive information be encrypted as well with an agency approved encryption technology.
- Users shall not use personal e-mail accounts (e.g. Hotmail, Gmail, etc.) for transmitting or receiving agency data, files or conducting agency business.
- Users shall have no expectation of privacy when using agency e-mail.
- Users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of any HHS agency or any unit of an HHS agency unless appropriately authorized to do so.
- Individuals must not send, forward, or receive HHS Confidential Information through non-HHS e-mail accounts, such as Yahoo, Hotmail, or Gmail.
- Users should not send or forward chain letters.
- Users should not send unsolicited messages to large groups except as required while conducting department business.

Instant Messaging

- The only approved Instant Messaging (IM) system is HHS provided Instant Messaging from Microsoft. Use of other Instant Messaging systems is prohibited except for specific instances approved by an IRM for HHS Agency business purposes.
- Policies relating to Instant Messaging can be found in the *HHS Policy for Use of Agency-Provided Instant Messaging*[2].

Internet

- Users will not utilize unapproved cloud computing resources or storage unless approved by HHS. These include but are not limited to Apple iCloud, Dropbox, Google Docs, or any other commercially available cloud computing service that is not expressly approved by HHSC IT.
  Internet access is provided to Users for agency business purposes, with limited incidental personal use allowed. Users shall only use agency approved services for file sharing of any form or method.
- Users shall not use personal or public available proxy server/devices to circumvent security policies for internet browsing.
- All software used to access the Internet must be approved for use on HHS IR.
- All software used to access the Internet must incorporate up-to-date vendor provided security patches.

[2] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

- All files downloaded from the Internet must be scanned for viruses using the approved HHS virus detection software with up to date signatures.
- All files downloaded from the Internet must fall within the defined download parameters allowed by the *HHS Information Security Policy (IS-Policy)*.
- No offensive or harassing materials may be accessed or posted to any Internet site using HHS IR.
- Internet access provided by HHS may not be used for personal solicitation or gain.

Incidental and Limited Personal Use

- Limited personal use of HHS IR is allowed for employees and other approved Users only. This use does not extend to visitors or relatives of the approved User.
- Limited use must not result in any additional direct costs to HHS.
- Limited use must not interfere with the normal performance of the User's duties.
- Limited personal use cannot violate any existing law or HHS policies.
- Storage of personal e-mail, voicemail, files, and any other document by the User on HHS IR must be kept to a minimum.
- All messages, files, and documents located on any HHS IR are owned by HHS and may be accessed by authorized HHS staff without notice to the User. Such documents may be subject to open records requests. This includes any personal messages, files, and documents.
- Incidental personal use of Internet access is permitted, but must not inhibit or interfere with the use or functionality of network resources for business purposes.
- Incidental, non-work related use of social networking sites such as Facebook, Myspace, Twitter, and videohosting sites such as YouTube are prohibited.
- Exceptions for the use of social media sites for approved HHS business purposes must be approved by their agency's Office of Communications or an employee designated by the agency's Commissioner to authorize social media use before establishing each new social media presence on the agency's behalf[3].

Remote and Virtual Private Network (VPN) Access

- Remote access to the HHS network shall be reviewed and approved by the appropriate supervisor. All employees by default shall have account settings set to deny remote access. Only upon approval shall the account settings be changed to allow remote access.
- Users that are authorized to telework or access HHS IR through remote access technology, (e.g., Virtual Private Network (VPN), Go to My PC, Outlook Web access) shall follow security practices that are the same as or equivalent to those required at their primary workplace.
- All (VPN) connections to HHS networks must be agency approved
- VPN access, granted by request to HHS, is a "User managed" service. Each User is responsible for obtaining their own Internet Service Provider (ISP).
  User supplied equipment connected to the VPN is subject to the policies, standards, controls, and guidelines that apply to HHS owned equipment.
- It is the User's responsibility, when connected to HHS networks via VPN, to assure that unauthorized Users are not allowed access to the HHS networks through the VPN connection.
- Any computing device connected to HHS networks must be protected by the use of a firewall that meets HHS security policy, standards, and controls.
- Any computing device connected to HHS networks or any other HHS technology must use anti-virus software and configurations approved by HHS IT.

[3] http://www.hhsc.state.tx.us/news/circulars/C-042.shtml

- VPN connections will be automatically disconnected after a period of non-use or inactivity. In this event, the User must log in again. The use of any technology to maintain an inactive connection (ping, stay-connect, etc.) is prohibited and can result in termination of the VPN account.
- Users of any computing device not owned by HHS must configure that device to comply with all HHS policies, standards, controls, and guidelines while connected to the HHS networks.
- The use of any VPN client not provided by HHS or its service provider is prohibited.
- The VPN User and IR are subject to audit to insure compliance with HHS policies, standards, controls, and guidelines.

Removable Media

- All HHS portable or removable media containing confidential information must be password protected and encrypted with an approved FIPS 140-2 cryptographic module.
- Confidential information, including ePHI that is stored on removable media or in paper form that is being transported to another location, must be labeled as confidential according to agency requirements. There must be a return address, and the media must be physically handed off and signed for, and tracked until it reaches its final destination, based on agency management risk decision. This includes facsimiles and printed materials sent by postal service or courier such as the United States Postal Service, FedEx, United Parcel Service of America (UPS), Mailmax, and agency or personal vehicles.
- In the event of loss or theft of removable media containing agency sensitive or confidential information, a description of the data and index or table of contents must be provided with the report of loss to the user's supervisor/ manager, the agency Information Security Officer and other agency or HHS offices as applicable, as further defined in the HHS Incident Response Plan. All removable media must be scanned for malicious code prior to use on HHS IR.
- Re-use or disposal of removable media must use a sanitization technique of clearing, purging, cryptographic erase, and/or destruction for agency sensitive or confidential information that meets HHS security policy, standard, and control requirements.

Mobile and Non-Agency Owned IT Devices

The following is only applicable if your agency has a Bring Your Own Device (BYOD) program:

- The Bring Your Own Device (BYOD) program, if offered by your agency, is an opt-in (voluntary) decision and requires that your agency have certain control over a User's personal or non-HHS owned device (smartphone, tablet, or laptop) in exchange for access to HHS Confidential Information or Information Resources such as the network and email. Users may opt-out of the BYOD program at any time.
- Users must meet BYOD eligibility, device requirements, and obtain management approval in order to participate in the BYOD program.
  HHS has no responsibility for User BYOD devices and associated costs, to include, but not limited to, vendor terms and conditions; sufficient data and call plan, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. Users are also responsible for the purchase, loss, damage, insurance, and/or replacement.
- Users will notify the help desk immediately if their BYOD device is lost or stolen, if there is a security incident associated with their device containing HHS information, or if there are plans to replace or sell their BYOD equipment so it can be removed from the approved list and remotely wiped. Additionally, Security incidents shall be immediately reported to the user's supervisor/ manager, the agency Information Security Officer and other agency or HHS offices as applicable, as further defined in the HHS Incident Response Plan.
- HHS can utilize information on a BYOD device as it determines is required or would be helpful to the organization to gather data on usage of mobile devices; ensure compliance with organization policies; gather

information for internal investigations or review; and to respond to information requests in litigation or government investigations.

- If a User is a Fair Labor Standards Act (FLSA) nonexempt employee, performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time, they are required to log all hours worked as required and prescribed by the applicable HHS's Human Resources (HR) policy.
- Supervisors of FLSA Non Exempt employee's will assure that FLSA Non Exempt employee's performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time will not be required to work after their assigned hours.
- Non-Agency Owned IT Devices must comply with all HHS security policy, standards, and controls.
- Operating Systems utilized must be on the HHS approved platforms supported list.
- Devices must be regularly scanned for malware and be running an HHS approved up-to-date anti-virus/antimalware software.
- HHS information must be encrypted and the encryption solution must meet HHS standards and controls, including the backup of Non-Agency Owned IT Devices.
- Device configuration must be compliant with HHS requirements, including the installation of HHS configuration management agent software.
- Users will comply with all agency requirements for securing HHS data.
- HHS reserves the right to review, retain or release personal and HHS-related data on Non-Agency Owned IT Devices during an investigation.
- In the event an HHS agency initiates a Non-Agency Owned IT Device wipe, the HHS agency expressly disclaims liability for any consequential loss of personal data or information stored on the device.
- Additional information on employee responsibilities associated with the BYOD program can be found on the IT policy website[4]

Physical Security

- Any User of HHS IR who takes the resource off-site to an environment out of the authority of HHS must follow the same information security policies, standards, controls, and guidelines to protect the resource as required when in use at an HHS location.
- Users will not use, disclose, transmit, maintain, create or remove Information Resources or HHS Confidential Information or HHS Agency sensitive information from HHS property without proper prior authorization and approval of supervisory HHS staff.
- Computer devices that display sensitive or confidential information should be positioned to prevent unauthorized access or viewing of information on the display.
- Users must use appropriate safeguards to protect IR from damage, loss or theft.
  Users will keep HHS IR under their physical control at all times, or will secure it in a suitable locked container under their control.
- Users will not leave HHS IR in their vehicle unattended.
- Users are required to ensure that all sensitive or confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked, logged out, or turned off when workspace is unoccupied.
- File cabinets containing confidential or sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to confidential or sensitive information must not be left at an unattended desk.
- Laptops, tablets, and other portable computing devices must be either locked with a locking cable or locked away in a drawer when left unattended.
- Printouts containing confidential or sensitive information should be immediately removed from the printer.

[4] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

- Confidential and sensitive documents should be placed in the locked confidential disposal bins when ready for disposal.
- Whiteboards containing confidential or sensitive information should be erased when not in use.
- Access mechanisms to secured facilities and key-cards must not be shared or loaned.
- Access mechanisms and key-cards that are no longer required must be returned to the appropriate HHS representative. Under no circumstances is a "retired" card to be passed directly to another User.
- Security incidents, including loss or theft of any Information Resource or information, shall be immediately reported to the user's supervisor/ manager, the agency Information Security Officer and other agency or HHS offices as applicable, as further defined in the HHS Incident Response Plan
- Lost or stolen access key-cards must be reported to the appropriate facility manager immediately upon the User becoming aware of the loss.

Confidential Information and Encryption

- Users shall ensure that they follow the requirements in the HHS Data Classification Standard when handling, processing or managing HHS information in electronic or physical format (e.g. printed documents).
- Users shall protect confidential information with encryption at rest and in motion. This includes encrypting confidential information when sending emails outside the HHS network.
- Users shall utilize only HHS approved encryption methods.
- Users are responsible for the protection of all sensitive or confidential information to which they may have access, either as a granted right or by accidental exposure.
- Users will protect sensitive and confidential information from disclosure to unauthorized persons or groups.
- Back-up storage media shall be protected in accordance with the highest level of sensitivity of the information being stored.
- Any User who becomes aware of or suspects an actual or possible incident of unauthorized access of confidential information must report such to the Help Desk, agency Information Security Officer (ISO) and agency Privacy Officer or designees immediately upon discovery. Additional documentation may also be required.
- Upon discovery of a possible unauthorized inspection or disclosure of Internal Revenue Service (IRS) Federal Tax Information (FTI) including breaches and security incidents, the individual making the observation or receiving the information should contact HHSC IRS Coordinator, at (512.206.5474). If you are unable to reach the HHSC IRS Coordinator by phone, send a secure e-mail to HHSC IRS FTI at IRS_FTI_Safeguards@hhsc.state.tx.us.
- Violation of the Data Classification Standard may result in disciplinary action which could include dismissal or suspension. Additionally, individuals are subject to loss of HHS Information Resources access privileges, and to civil and criminal prosecution.

Media Disposal

- Users should consult with their Information Security Office for instruction on performing the correct media sanitization procedures as defined in this section.
- Users shall perform media sanitization prior to disposal, release out of HHS organizational control, or release for reuse using sanitization techniques in accordance with applicable federal, state, and organizational standards and policies.
- Users shall ensure proper disposal (purging and destruction) of digital and non-digital information system media.
- Users shall ensure that the information system media is sanitized or destroyed before disposal or release for reuse.

- Re-use or disposal of media must use a sanitization technique of clearing, purging, cryptographic erase, and/or destruction for agency sensitive or confidential information that meets HHS security policy, standard, and control requirements.

Monitoring of Information Resources

- HHS has the legal right to monitor use of HHS Information Resources, HHS Confidential Information, and HHS Agency sensitive information and HHS monitors use to ensure these resources are protected and to verify compliance with applicable law, HHS Policy, security standards and controls. By using HHS Information Resources, or using, disclosing, creating, transmitting, or maintaining HHS Confidential Information or HHS Agency sensitive information, users consent to the monitoring of the use of these resources and information in any form and on any device and understand there is no expectation of privacy.
- Users are notified of monitoring through various means:
    - Signing the Health and Human Services Acceptable Use Agreement (AUA)
    - Warning banners on electronic devices
    - Information security awareness publications and training
    - HHS security policy, standards, controls, guidelines, and procedures (ISSG, IS-Policy, etc.).

Compliance

- Non-compliance or violation of the HHS Information Security Acceptable Use Policy (AUP) may be cause for removal of access and disciplinary action, up to and including dismissal and/or civil or criminal prosecution. Users also must comply with applicable law and HHS Agency policies, procedures, standards and guidelines over Information Resources, HHS Confidential Information, and HHS Agency sensitive information such as the requirements in the HHS Human Resources Manual, HHS Privacy Policy and HHS Security Policy, as well as any changes to those requirements.
- Depending on the severity of the violation, consequences may include one or more of the following actions:
    - Immediate suspension of access privileges and revocation of access to HHS Information Resources, HHS Confidential Information or HHS Agency sensitive information;
    - Disciplinary action, up to and including dismissal;
    - Removal or debarment from work on HHS contracts or projects;
    - Civil monetary penalties; and/or
    - Criminal charges that may result in imprisonment for misuse of HHS Information Resources or Confidential Information.

For more information or to provide comments please contact *InfoSecurity@hhsc.state.tx.us*

Exhibit D: Health and Human Services Acceptable Use Agreement (AUA):

Health and Human Services Acceptable Use Agreement (AUA)

(Formerly known as the Computer Use Agreement or CUA)

Please read the following agreement carefully and completely before signing.

Purpose

The purpose of this document is to inform you of your responsibilities concerning the use of Texas Health and Human Services System (HHS) Confidential Information, HHS Agency sensitive information, and HHS Information Resources.[1] This includes: computer, hardware, software, infrastructure, data, personnel, and other related resources. Your signature is required to formally acknowledge your understanding, acceptance, and compliance of HHS's Information Resource Acceptable Use provisions. This agreement applies to all persons using HHS Information Resources and/or using, disclosing, creating, transmitting, or maintaining HHS Confidential Information or HHS Agency sensitive information, whether employed by an HHS Agency or not, and is based on policy delineated in the HHS Enterprise Information Security Policy (EIS-Policy), and the HHS Enterprise Information Security Acceptable Use Policy (EIS-AUP). Users are further informed of their responsibilities regarding the use of HHS Information Resources when taking the required annual *HHS Enterprise Information Security Acceptable Use Training.*

I understand and hereby agree to comply with the following Information Resource Acceptable Use provisions:

Authorized Use

- Information Resources are intended to be used in support of official state-approved business.
- Limited personal use of Information Resources may be allowed and is described in other policies and procedures of the HHS Agency by which I am employed.
- Proper authorization is required for access to all information owned by HHS Agencies, except for information that is maintained for public access.
- I will not attempt to access or alter any information that I am not authorized to work with in the performance of my job duties.
- I will not enter any unauthorized information, make any unauthorized changes to information, or disclose any information without proper authorization. Unauthorized access to an HHS Information Resource, allowing another party unauthorized access to, or maliciously causing a computer malfunction are violations under Chapter 33 of the Texas Penal Code ("Computer Crime Law") and are punishable by fines, jail time, or both.

User Credentials

- I will receive and will be required to use credentials (User ID and Password) to gain access to and to use HHS Information Resources.
- I will employ a difficult to guess password with a minimum of eight characters in length containing upper case alpha, lower case alpha, numerical, and special characters unless further requirements for passwords are issued.
- I will not construct my password from obvious user names or passwords, such as personal information (i.e. telephone numbers, relative's names, pet's names, or passwords used for personal business, etc.).
- Under no circumstances will I allow my credentials to be used by any other individual, nor will I use

[1] As defined in HHS EIS-Definitions document:
§2054.003(7), Texas Government Code.
Information resources" means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.
And as defined in [44 U.S.C., Sec. 3502], NIST SP 800-53 rev 4.
Information and related resources, such as personnel, equipment, funds, and information technology.

credentials belonging to someone else.

- I will be held responsible for any violations of applicable law or agency policy related to HHS Confidential Information, HHS Agency sensitive information, or HHS Information Resources, caused by my acts or omissions, or for any harm, loss, or adverse consequences arising from the use of my credentials, including any unauthorized use by a third party or contractor if such party gains access to my credentials due to my negligence or misconduct. Disciplinary actions up to and including dismissal and civil or criminal prosecution may result from any violations or misuse.
- Transactions initiated under my credentials will be considered as having been authorized and electronically signed by me.
- I will not disclose my password to anyone.

Software

- Only properly licensed software may be used on HHS Information Resources.
- I will use all software installed on HHS Information Resources in a manner that complies with the terms of the applicable software license agreement and all applicable law and HHS Agency policies and procedures.
- I will not install or use any software on HHS Information Resources that has not been approved for use in accordance with HHS Agency policies and procedures.

HHS Confidential Information

HHS Confidential Information includes information from the IRS (Federal Tax Information (FTI)) or the Social Security Administration (SSA), personally identifiable information, such as patient/client identifying health information, employee information, unpublished agency work product, or any information (patient or otherwise) that is classified confidential by applicable law and HHS Agency policy. You may have authority to use or disclose some or all of this HHS Confidential Information only as an authorized person through a computer system, or in paper or oral form or for your work for authorized purposes.

HHS Confidential Information is valuable and sensitive, and is protected by law and by HHS policies. The intent of these laws and policies is to safeguard the information against unauthorized use or disclosure and in support of the organization's mission. As a user of HHS systems and HHS Confidential Information, you are required to conform to applicable laws and HHS policies governing confidential information. Your principal obligations in this area are outlined below. You are required to read and to abide by these obligations.

I understand that in the course of my job, I may have authority to use or disclose HHS Confidential Information related to:

- Individuals' personally identifiable information about patients/clients (such as records, conversations, admissions information, diagnosis, prognosis, treatment plan, financial information, or other identifiers such as name, social security number, benefit plan, etc.) HHS Workforce personally identifiable information including home addresses, home phone numbers, and social security numbers. HHS Workforce includes employees, interns, trainees, volunteers, and staff augmentation contractors.
- HHS Agency functions (such as unpublished or draft financial information, internal reports, memos, contracts, peer review information, communications, proprietary computer software, and procurement information).
- Legal work product or other information deemed confidential under applicable law or HHS Agency policy.
- Contractor or third party information (such as vendor information).

Accordingly, as a condition of my access to HHS Confidential Information, I agree that:

- I will use HHS Confidential Information only as needed to perform legitimate duties. This means, among other things, that:

- I will only access HHS Confidential Information that I have a need to know;
- I will not in any way create, use, disclose, transmit, maintain, copy, sell, loan, review, alter, or destroy any HHS Confidential Information except as properly authorized within the scope of my duties for HHS;
- I will not misuse or carelessly handle HHS Confidential Information; and
- I will encrypt HHS Confidential Information when appropriate, including when emailing such information and when storing such information on portable storage devices. I will not use confidential individual identifiers in email subject lines because subject lines are never encrypted.
- I will safeguard and will not disclose my user name or password or any other authorization I have that allows me to access to HHS Confidential Information, except as permitted by law and applicable HHS Agency policy.
- I will report activities by any other individual or entity that I suspect may compromise the confidentiality, integrity or availability of HHS Confidential Information to my supervisor and the HHS Privacy Office at: privacy@hhsc.state.tx.us or (877) 378-9869 or the agency's Privacy Office. I will immediately report computer security incidents to the help desk.
- Reports are made in good faith about suspect activities and will be held in confidence to the extent permitted by law, including the name of the individual reporting the activities. Retaliation for a good faith report of a violation of law or policy is prohibited by HHS.
- My obligations under this Agreement will continue after termination of my association with HHS or access to HHS applications until all HHS Confidential Information in my possession, custody or control is returned or destroyed as directed by HHS.
- My privileges hereunder are subject to periodic review, revision, and if appropriate, removal.
- I have no right or ownership interest in any HHS Confidential Information referred to in this Agreement. HHS may revoke my access code or other authorized access to HHS Confidential Information at any time.
- I will, at all times, safeguard and retain the confidentiality, integrity and availability of HHS Confidential Information.
- I acknowledge my responsibility to be aware of, read, and comply with HHS security policy, standards, and controls[2].

Agency Sensitive Information

Agency sensitive information is information that is not subject to specific legal, regulatory or other external requirements, but is considered HHS sensitive and should not be readily available to the public. Agency sensitive information must be protected even though disclosure is not specifically restricted by legal or regulatory requirements.

Examples of agency sensitive information include but are not limited to:

- HHS-specific legal information such as nondisclosure agreements (NDAs) and contracts.
- Unpublished financial information related to organizational accounting such as balance sheets, purchase orders, contracts and budget information.
- Unpublished financial information related to employee compensation, such as offer letters, salaries, severance, retirement plans, and benefits.
- Internal operational procedures.

Some information, even though it is available to the public, may contain sensitive information. Consequently, I understand it is also my responsibility to protect this information according to its sensitivity, value, and impact to HHS.

I understand that my failure to comply with this Agreement may result in loss of access privileges to HHS applications; disciplinary action, up to and including dismissal; and civil or criminal prosecution.

If I receive a request for the public disclosure of information, I will follow my agency's policies and procedures for the release of public information.

[2] HHS security policy, standards, and controls can be found at http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

Health and Human Services
Acceptable Use Agreement (AUA)

(Formally known as the Computer Use Agreement or CUA)

Workforce Nondisclosure and Procurement Integrity Statement

As an HHS workforce member (employee, trainee, intern, volunteer or staff augmentation contractor) of the Texas Health and Human Services Commission (HHSC) or a Health and Human Services (HHS) agency, I may be provided access to HHS Confidential Information or agency sensitive information regarding the proposed work, procurement of goods and services for HHSC or an HHS Agency. As such, I acknowledge that:

- My access to this information is authorized only within my duties as an HHS Workforce Member of HHSC or an HHS Agency;
- My access to this information is solely for the purpose of discharging the duties of HHSC or an HHS Agency regarding the proposed procurement;
- Premature or unauthorized disclosure of this information will irreparably harm the State's interests in the proposed procurement and may constitute a violation of *Section 39.02 of the Texas Penal Code*, the antitrust laws of the United States and the State of Texas, and the *Texas Public Information Act, Chapter 552, Texas Government Code*; and
- The information may represent confidential or proprietary information, the release of which may be restricted or prohibited by law.

In view of the foregoing, I agree that I shall only use, disclose, create, maintain or transmit any information that I receive in my capacity as an HHS workforce member, in any form, whether electronic, paper or oral, formal or informal – for the following authorized purposes only:

- To provide the goods, services and/or deliverables required or requested under this HHSC or HHS Agency procurement in accordance with my assigned duties;
- To provide action, response or recommendation requested by HHSC or an HHS Agency in the course of fulfilling my assigned duties regarding the proposed procurement as prescribed under the resulting contract;
- To evaluate the submissions received from vendors or offerors in connection with the proposed procurements in accordance with my assigned duties;
- To assist HHSC or an HHS Agency in developing any documents, reports, working papers, evaluations, schedules, or instruments necessary to fulfill the requirements of the procurement; or
- As otherwise authorized in writing by HHS.

I further agree that I will regard any such information as confidential and that I will not use, disclose, create, transmit or maintain the information or any summary or synopsis of the information in any manner or any form whatsoever, except under the following circumstances:

- When authorized in writing by an HHSC or HHS employee associated with the respective proposed procurement or my assigned duties at HHS;
- When required by law as determined by HHS Legal Counsel;
- When the information has previously been released to the general public by HHSC or an HHS Agency regarding the respective proposed procurement -provided such release was not inadvertent or unintentional; and
- When required, to brief or inform a manager or supervisor, provided the manager or supervisor is informed of and agrees to the limitations on further disclosure contained in this statement.

In the event I receive a request for information relating to a proposed procurement either during or after the performance of this resulting contract, I agree to do the following:

- Notify HHSC or HHS Agency Information Owner associated with the respective proposed procurement as soon as practical following receipt of the request, who will seek advice from appropriate legal counsel and further instruct me regarding my ability to disclose the information.

The aforementioned statements supersede any other non-disclosure statement related to a proposed procurement or work duties. Any prior authorizations relating to access to information related to a proposed procurement are revoked.

In addition, I agree to notify the HHSC or HHS Agency employee associated with the respective proposed procurement immediately if I learn or have reason to believe that any information covered by this Workforce Nondisclosure and Procurement Integrity Section has been disclosed, intentionally or unintentionally, by any person.

Physical Security

- I will not use, disclose, transmit, maintain, create or remove Information Resources or HHS Confidential Information or HHS Agency sensitive information from HHS property without proper prior authorization and approval of supervisory HHS staff.
- I will immediately report the loss or theft of any Information Resource or information to the appropriate investigative office in accordance with all HHS Agency policies and procedures.
- I will secure my workstation either by logging off or locking my screen when away from my workstation.
- I will keep HHS Information Resources under my physical control at all times, or will safeguard them when away, such as by keeping my workspace clean, not leaving HHS Confidential Information, HHS Agency sensitive information, or Information Resources in my vehicle unattended and locking Information Resources with a locking cable or a suitable locked container under my control.

E-Mail

- I understand that the state government e-mail system is provided for official HHS business.
- I will limit my incidental, non-official use of the e-mail system to prevent interference with my official duties or cause degradation of network services, in accordance with HHS Agency policy.
- I will not send e-mail that violates HHS Agency policy, such as e-mail that contains malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or inappropriate racial, gender, sexual, or religious content over state government e-mail.
- I will not use personal email accounts (e.g. Gmail, Hotmail, Yahoo etc.) for transmitting or receiving HHS Agency information or conducting agency business.
- I will utilize HHS Agency approved encryption for transmitting HHS Confidential Information.

Internet

- I understand that access to public networks (i.e. the Internet) is for official HHS business.
- I will limit my incidental, non-official access to the Internet to prevent interference with my official duties or cause degradation of network services, in accordance with HHS Agency policy.
- I will not view or attempt to view web content that violates HHS policy, such as sites known to contain malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or inappropriate racial, gender or sexual content, text or graphics.
- I will not utilize unapproved cloud computing resources or storage unless approved by HHS. These include but are not limited to Apple iCloud, Dropbox, Google Docs, or any other commercially available cloud computing service that is not expressly approved by HHSC IT.
- I will not use a personal or public available proxy to circumvent security policies for internet usage.

Social Media

I understand from the HHS Social Media Policy, that incidental, non-work related use of social networking sites such as Facebook, Myspace, Twitter, and video-hosting sites such as YouTube are prohibited. Exceptions for the use of social media sites for approved HHS business purposes must be approved by their agency's Office of Communications or an employee designated by the agency's Commissioner to authorize social media use before establishing each new social media presence on the agency's behalf.

Instant Messaging

I understand that the only approved Instant Messaging (IM) system is HHS provided Instant Messaging from

Microsoft. Use of other Instant Messaging systems is prohibited except for specific instances approved by an Information Resources Manager (IRM) for HHS Agency business purposes. Policies relating to Instant Messaging can be found in the *HHS Policy for Use of Agency-Provided Instant Messaging*[3].

Non-Agency Devices

The following is only applicable if your agency has a Bring Your Own Device (BYOD) program:

I understand the Bring Your Own Device (BYOD) program, if offered by my agency, is an opt-in (voluntary) decision and requires that my agency have certain control over my personal or non-HHS owned device (smartphone, tablet, or laptop) in exchange for access to HHS Confidential Information or Information Resources such as the network and email. I may opt-out of the BYOD program at any time.

I must meet Bring Your Own Device (BYOD) eligibility, device requirements, and obtain management approval in order to participate in the BYOD program.

I understand HHS has no responsibility for my BYOD devices and associated costs, to include, but not limited to, vendor terms and conditions; sufficient data and call plan, service levels, calling areas, service and phone features, termination clauses, and payment terms and penalties. I am also responsible for the purchase, loss, damage, insurance, and/or replacement.

I will notify the help desk immediately if my BYOD device is lost or stolen, if there is a privacy or security incident associated with my device containing HHS information, or if there are plans to replace or sell my BYOD equipment.

I understand that HHS, at its sole discretion, can utilize information on a BYOD device as it determines is required or would be helpful to the organization to gather data on usage of mobile devices; ensure compliance with organization policies; gather information for internal investigations or review; and to respond to informational requests in litigation or government investigations.

I understand that if I am a Fair Labor Standards Act (FLSA) nonexempt employee, performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time, that I am required to log all hours worked as required and prescribed by the applicable HHS's Human Resources (HR) policy.

I understand that if I am a Supervisor of FLSA Non Exempt employee's, I will assure that FLSA Non Exempt employee's performing work under the BYOD or other program or technology that makes accessing work convenient from any location or time will not be required to work after their assigned hours unless directed by their supervisor or manager.

Additional information on employee responsibilities associated with the BYOD program can be found on the IT policy website[4].

Consent to Monitoring

I understand that HHS has the legal right to monitor use of HHS Information Resources, HHS Confidential Information, and HHS Agency sensitive information and that HHS monitors use to ensure these resources are protected and to verify compliance with applicable law, HHS Policy, security standards and controls. By using HHS Information Resources, or using, disclosing, creating, transmitting, or maintaining HHS Confidential Information or HHS Agency sensitive information, I consent to the monitoring of the use of these resources and information in any form and on any device and understand I have no expectation of privacy.

[3] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

[4] http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

Health and Human Services
Acceptable Use Agreement (AUA)

(Formally known as the Computer Use Agreement or CUA)

Non-Compliance

I understand that non-compliance with this agreement or violation of the HHS Enterprise Information Security Acceptable Use Policy (AUP) may be cause for removal of access and disciplinary action, up to and including dismissal and/or civil or criminal prosecution. I also understand that I must comply with applicable law and HHS Agency policies, procedures, standards and guidelines over Information Resources, HHS Confidential Information, and HHS Agency sensitive information such as the requirements in the HHS Human Resources Manual, HHS Privacy Policy and HHS Security Policy, as well as any changes to those requirements.

Depending on the severity of the violation, consequences may include one or more of the following actions:

- Immediate suspension of access privileges and revocation of access to HHS Information Resources, HHS Confidential Information or HHS Agency sensitive information;
- Disciplinary action, up to and including dismissal;
- Removal or debarment from work on HHS contracts or projects;
- Civil monetary penalties; and/or
- Criminal charges that may result in imprisonment for misuse of HHS Information Resources or HHS Confidential Information.

USER MUST ACKNOWLEDGE ALL PAGES OF THIS AGREEMENT.

I have read, understand and agree to comply with this agreement.

HHS Employee Signature: _____

HHS Contractor Signature: _____

HHS Employee/Contractor Name Printed: _____

HHS Employee ID: _____

HHS Agency and Department or Division: _____

Date Agreement Signed _____

For the purpose of this document, "HHS", "HHS Agency", or "HHS Agencies" include the Health and Human Services Commission, Department of Aging and Disability Services, Department of Family and Protective Services, Department of State Health Services, Department of Assistive and Rehabilitative Services, and/or any successor agency or component part thereof.

Definitions can be found in the HHS Enterprise Information Security Definitions (http://hhscx.hhsc.texas.gov/it/policies-and-guidelines), HHS Privacy Policies and Procedures and the HHS Human Resources Manual (http://hhscx.hhsc.state.tx.us/hr/HRM/contents.htm).

Exhibit E: HHS System Data Use Agreement

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. All of Contractor's Authorized Users, Workforce and Subcontractors with access to a state computer system or database will complete a cybersecurity training program certified under Texas Government Code Section 2054.519 by the Texas Department of Information Resources.

(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/laws-regulations/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: _____

HHS Data Use Agreement v. 8.5

Exhibit E-1: HHS System 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 H H S 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 F: Experience Reference Form

HHS0004417 – Exhibit F

Project and Portfolio Management Configuration & Implementation Services

– Experience Reference Form

Project Information:	
Vendor Name:	Vendor Contact/Name:
Project Dates:	Vendor Contact Phone:
Customer Organization:	Customer Contact Name:
	Customer Phone:
Customer Address:	Customer Fax:

Vendor (Prime Contractor or Subcontractor) has performed PPM Implementation and Configuration with Data Migration services of similar size and complexity within the last five (5) years for a paying customer external to the Vendor's organization: Yes No

Project Objectives and Deliverables Description

Vendor's Involvement:

Project Benefits (Quantitative):

Planned:

Realized:

Project Benefits (Qualitative):

Planned:

Realized:

What Tools and Technologies were recommended for the solution?

Were the Recommendations Implemented by the Customer? Yes No

Who can we contact at the customer regarding the implementation of the recommendations for the data analytics and performance management solution?

Customer Contact:
Name: _____ Phone _____
Email: _____

Project Measurements:				
Original Value of Vendor's Contract:		Actual Total Contract Value:		
Reason(s) for Change in Value:				
Estimated Start & Completion Dates:	From:		To:	
Actual Start & Completion Dates:	From:		To:	
Reason(s) for Difference Between Estimated and Actual Dates:				

Page 2 of 2

Exhibit F-1: RESPONDENT RELEASE OF LIABILITY

THIS FORM MUST BE COMPLETED/SIGNED BY RESPONDENT FOR EACH IDENTIFIED REFERENCE AND SUBMITTED WITH THE RESPONDENT'S RESPONSE SUBMISSION

Legal name of company or government entity identified as a reference by respondent vendor ("*Reference Customer*"):

Enter name of company providing the reference here

Respondent vendor ("*Respondent*") full legal name (include *dba* if applicable for this reference):

Enter name of company (Respondent) or key staff person's name needing a reference

Entity directed by Respondent to contact the Reference Customer designated above:

Texas Health and Human Services Commission ("*HHSC*")

By signing below, the Respondent (and, if applicable, individual key staff person(s) signing below) hereby irrevocably releases the above-named Reference Customer, its officers, directors, agents, employees, and all persons, natural or corporate, in privity with above-named Reference Customer from any and all liability, claims, or causes of action, under any theory and whether foreseeable or unforeseeable, arising from or out of their disclosure of information to HHSC pursuant to this request for a business reference.

Signed the _____ day of _____, 20____.

_____
(Respondent Signature)

_____
(Respondent Printed Name)

_____
(Respondent Title)

Signed the _____ day of _____, 20____.

_____
(Key Staff Signature or "N/A" if Respondent-level release)

_____
(Key Staff Printed Name)

Exhibit G – Vendor Price Sheet

Deliverable Costs:

List each deliverable, the cost associated to that deliverable, a 10% retainage, and the net deliverable payable monthly upon acceptance.

Deliverable No.	Deliverable	Deliverable Cost	Retainage	Net Deliverable
D.1.1	Project Work Plan			
D1.2	Communication Plan & Escalation Strategy			
D1.3	Knowledge Transfer Plan			
D1.4	PPM Installation Checklist			
D1.5	PPM Configuration Documentation and updates throughout project			
D1.6	Functional Design (Word/Excel)			
D1.7	Process Workflows (Visio)			
D1.8	Requirements and user stories			
D1.9	End User Testing Acceptance			
D1.10	Migration Plan			
D1.11	Conversion Plan			
D1.12	Converted data into PPM from Dovico, Salesforce & BASS OIG-IT time reporting applications			
D1.13	Migrated data into PPM from FY (Fiscal Year) Planning and PMRS (Project Management Reporting System)			
D1.14	Requirements Traceability Matrix			
D1.15	Training Plan			
D1.16	Administrator Training Package			
D1.17	Operator/User Training Package			
D1.18	Mobile time reporting (phone or tablet)			
D1.19	Load Testing			
D1.20	Security Compliance			
D1.21	Phase Closeout			
D1.22	TIERS related work			
	Total	$	$	$

Deliverable No.	Deliverable	Deliverable Cost	Retainage	Net Deliverable
D2.1	Requirements Traceability Matrix			
D2.2	One-way interface for CAPPS to feed into PPM			
D2.3	One-way interface for PPM audit logs to feed into Splunk			
D2.3	System Integration Testing (SIT)			
D2.4	End to End (E2E) Solution Testing			
D2.5	Load Testing			
D2.6	Security Compliance			
D2.7	End User Testing			
D2.9	Utility to remove the records no longer required as defined by the HHSC records retention requirements listed in **Exhibit I-1**.			
D2.10	Plug-in for MS Project			
D2.11	Phase Closeout			
D2.12	TIERS related work			
	Total	$	$	$

Deliverable No.	Deliverable	Deliverable Cost	Retainage	Net Deliverable
D3.1	PPM Configuration Documentation and updates throughout project			
D3.2	Updated PPM Installation Checklist			
D3.3	Functional Design (Word/Excel)			
D3.4	Process Workflows (Visio)			
D3.5	Updated Requirements Traceability Matrix			
D3.6	End User Testing Acceptance			
D3.7	Administrator Training Package			
D3.8	End User Training Package			
D3.9	System Integration Testing			
D3.10	End to End Testing			
D3.11	Load Testing			
D3.12	Security Compliance			
D3.13	Phase Closeout			
D3.14	TIERS related work			
	Total	$	$	$

.

Deliverable No.	Deliverable	Deliverable Cost	Retainage	Net Deliverable
D4.1	Reports (20 custom reports)			
D4.2	Updated Requirements Traceability Matrix			
D4.3	Phase/Project Closeout			
D4.4	TIERS related work			
	Total	$	$	$

Deliverable No.	Deliverable	Deliverable Cost	Retainage	Net Deliverable
	Grand Total	$	$	$

Exhibit H – HHSC Uniform Terms and Conditions

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

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 non-enforceability 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.

8.17 Dispute 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.

8.23 Counterparts

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 H-1 – HHSC Special Conditions

Health and Human Services Commission
Special Conditions
Version 1.2
9.1.17

Contents

Article I. Special Definitions **1**

Article II. General Provisions **2**

[redacted] 2

[redacted] 2

Section 2.01 Other System Agencies Participation in the Contract 2
Section 2.02 Most Favored Customer 2
Section 2.03 Cooperation with HHSC Vendors 3
Section 2.04 Renegotiation and Reprocurement Rights 3

Article III. Contractors Personnel and Subcontractors **3**

Section 3.01 Qualifications 3
Section 3.02 Conduct and Removal 3

Article IV. Performance **4**

Section 4.01 Measurement 4

Article V. Amendments and Modifications **4**

Section 5.01 Formal Procedure 4
Section 5.02 Minor Administrative Changes 4

Article VI. Payment **4**

Section 6.01 Enhanced Payment Procedures 4

Article VII. Confidentiality **5**

Section 7.01 Consultant Disclosure 5
Section 7.02 Confidential System Information 5

Article VIII. Disputes and Remedies **6**

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

Article IX. Damages **7**

Section 9.01 Availability and Assessment 7
Section 9.02 Specific Items of Liability 7

Article X. Turnover **8**

Section 10.01 Turnover Plan 8
Section 10.02 Turnover Assistance 8

Article XI. Additional License and Ownership Provisions **8**

Section 11.01 HHSC Additional Rights 8
Section 11.02 Third Party Software 9

Section 11.03 Software and Ownership Rights 9

Article XII. Uniform ICT Accessibility Clause 9

Section 12.01 Applicability 9
Section 12.02 Definitions 9
Section 12.03 Accessibility Requirements 10
Section 12.04 Evaluation, Testing and Monitoring 10
Section 12.05 Representations and Warranties 11
Section 12.06 Remedies 11

Article XIII. Miscellaneous Provisions 12

Section 13.01 Conflicts of Interest 12
Section 13.02 Flow Down Provisions 12
Section 13.03 Manufacturer's Warranties 12

Article XIV. DSHS Legacy Provisions 13

Section 14.01 Notice of Criminal Activity and Disciplinary Actions 13
Section 14.02 Notice of IRS or TWC Insolvency 13
Section 14.03 Education to Persons in Residential Facilities 13
Section 14.04 Disaster Services 13
Section 14.05 Consent by Non-Parent or Other State Law to Medical Care of a Minor 14
Section 14.06 Telemedicine /Telepsychiatry Medical Services 14
Section 14.07 Services and Information for Persons with Limited English Proficiency 14
Section 14.08 Third Party Payors 15
Section 14.09 HIV/AIDS Model Workplace Guidelines 15
Section 14.10 Medical Records Retention 15
Section 14.11 Notice of a License Action 15
Section 14.12 Interim Extension Amendment 16
Section 14.13 Child Abuse Reporting Requirement 16

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.

"**Other 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 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.

"**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.

"**Turnover**" means the effort necessary to enable HHSC, or its designee, to effectively close out the Contract and move the Work to another vendor or to perform the Work by itself.

"**Turnover Plan**" means the written plan developed by Contractor, approved by HHSC, and to be employed when the Work described in the Contract transfers to HHSC, or its designee, from the Contractor.

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

Article II. General Provisions

2.01 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.

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 SOW, 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 Services, 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. PAYMENT

5.01 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 VI. CONFIDENTIALITY

6.01 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.

6.02 Confidential System Information

HHSC prohibits the unauthorized disclosure of Other Confidential Information. Contractor and all Contractor Agents will not disclose or use any Other Confidential 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 Other Confidential Information. Any disclosure or transfer of Other Confidential Information by Contractor, including information requested to do so by HHSC, will be in accordance with the Contract. If Contractor receives a request for Other Confidential Information,

Contractor will immediately notify HHSC of the request, and will make reasonable efforts to protect the Other Confidential 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 Other Confidential 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 Other Confidential 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 OTHER CONFIDENTIAL INFORMATION. Contractor WILL FULFILL THIS PROVISION WITH COUNSEL APPROVED BY HHSC.

Article VII. Disputes and Remedies

7.01 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.

7.02 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: i) constitute a waiver of any other remedy that HHSC may have at law or equity; ii) excuse Contractor's prior substandard performance; iii) 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.

7.03 Equitable Remedies

Contractor acknowledges and agrees that if Contractor breaches, or 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, or 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.

7.04 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 VIII. DAMAGES

8.01 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.

8.02 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 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 IX. TURNOVER

9.01 Turnover Plan

HHSC may require Contractor to develop a Turnover Plan at any time during the term of the Contract in HHSC's sole discretion. Contractor must submit the Turnover Plan to HHSC for review and approval. The Turnover Plan must describes Contractor's policies and procedures that will ensure:

(a) The least disruption in the delivery the Work during Turnover to HHSC or its designee; and
(b) Full cooperation with HHSC or its designee in transferring the Work and the obligations of the Contract.

9.02 Turnover Assistance

Contractor will provide any assistance and actions reasonably necessary to enable HHSC or its designee to effectively close out the Contract and transfer the Work and the obligations of the Contract to another vendor or to perform the Work by itself. Contractor agrees that this obligation survives the termination, regardless of whether for cause or convenience, or the expiration of the Contract and remains in effect until completed to the satisfaction of HHSC.

Article X. UNIFORM ICT ACCESSIBILITY CLAUSE

10.01 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 publis 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/Recipeint 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.

10.02 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.

10.03 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.

10.04 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.
2. 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.
3. 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.

10.05 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.

10.06 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 XI. MISCELLANEOUS PROVISIONS

11.01 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.

11.02 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.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit I - Scope of Work Supporting Documents

Exhibit I-1 – Requirements

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
	Technical Topic	**Security & Auditing**		
T01.001	Security & Auditing	Have the ability to secure access via login and password	TBD	TBD
T01.002	Security & Auditing	Have the ability to set up delegates for approvals	TBD	TBD
T01.003	Security & Auditing	Have the ability to configure user preferences	TBD	TBD
T01.004	Security & Auditing	Have the ability to support self-service for username and password resets	TBD	TBD
T01.005	Security & Auditing	Have the ability to audit activity, record and report on record update history	TBD	TBD
T01.006	Security & Auditing	Provide access control for establishing projects	TBD	TBD
T01.007	Security & Auditing	Provide support for time allocation approval process (with audit trail)	TBD	TBD
T01.008	Security & Auditing	Provide ability to manage security separately for projects and programs	TBD	TBD
T01.009	Security & Auditing	Comply with all required security controls prior to moving into production or obtain an exception approval to not implement a specific security control	TBD	TBD
T01.010	Security & Auditing	Provide ability to lock time allocation entry following approval	TBD	TBD
T01.011	Security & Auditing	For all records associated with an audit, the retention period is to be after close of the audit + 10 years. These records are to be maintained online tor a period of 90 days and offline for 10 years. The data migration should include only those audit records that fall within the retention period defined.	TBD	TBD
T01.012	Security & Auditing	Ensure HIPAA security requirements are maintained throughout the implementation of the SaaS PPM application using FedRAMP and/or NIST 800-53.	TBD	TBD
T01.013	Security & Auditing	Export Auditable events to Splunk	TBD	TBD
	Technical Topic	**Compatibility & Integration**		
T02.001	Compatibility & Integration	Have the ability to integrate (bi-directionally) with other third-party software, such Microsoft Project, JIRA, salesforce, accounting software, project reporting tools, CAPPS, enterprise portal, ALM, Team Forge, FY Planning, TFS (Team Foundation Services - MS product) etc.	TBD	TBD
T02.002	Compatibility & Integration	Not used		
T02.003	Compatibility & Integration	Not used		
T02.004	Compatibility & Integration	Have the ability to be utilized on HHS IT approved web browsers	TBD	TBD
T02.005	Compatibility & Integration	Provide interface from CAPPS HR or financial warehouse to maintain resources (staff and contractors) available to the PPM resources available for assignment	TBD	TBD

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
T02.006	Compatibility & Integration	Not used		
T02.007	Compatibility & Integration	Have intuitive user interface for ease of use	TBD	TBD
T02.008	Compatibility & Integration	Eliminate duplicitous data entry	TBD	TBD
T02.009	Compatibility & Integration	Not used		
	Technical Topic	**Performance**		
T03.001	Performance	Have the ability to support ~5000 users	TBD	TBD
T03.002	Performance	Have ability to archive closed projects	TBD	TBD
T03.003	Performance	Maintain records based upon agency's record retention policies. Provide utility to run annually to remove records from the application that fall outside the retention periods defined in these requirements.	TBD	TBD
	Business Topic	**General**		
B01.001	General	Have the ability to auto-populate time allocation sheet with approved / allocated activities and projects and only allocate time to those that approved for a project/application	TBD	TBD
B01.002	General	Have the ability to allocate time for multiple days at once	TBD	TBD
B01.003	General	Have the ability to support variety of product development processes (waterfall, agile, iterative)	TBD	TBD
B01.004	General	Allow end user to allocate their time to projects in 15-minute increments	TBD	TBD
B01.005	General	Not used		
B01.006	General	Provide ability to import the existing projects portfolio	TBD	TBD
B01.007	General	Provide ability to create project groups and/or portfolios that can then be used for tracking and reporting purposes	TBD	TBD
B01.008	General	Provide ability to rank projects and proposals on one or more sets of criteria	TBD	TBD
B01.009	General	Not used		
B01.010	General	Generate post implementation assessment reminder	TBD	TBD
B01.011	General	Complies with accessibility standards	TBD	TBD
B01.012	General	Provide ability to establish and maintain calendars as an administrative activity	TBD	TBD
B01.013	General	Provide ability to document or tie to other requests (new and existing) and reference other request types (integrate requirements between resources, demand and other attribute types)	TBD	TBD
B01.014	General	Provide ability to establish period type (example: weekly, biweekly, semi-monthly, monthly)	TBD	TBD
B01.015	General	Provide external facing access	TBD	TBD

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
B01.016	General (TIERS)	Maintain customization for the Create Project button that automatically creates an associated project for a service request based on a user-selected Project Type and Work Plan Template.	TBD	TBD
B01.017	General (TIERS)	Maintain customization for the Create Project button that creates project for Releases.	TBD	TBD
	Business Topic	**Resource Management**		
B02.001	Resource Management	Provide ability to determine where resource time goes in a month. Identify characteristics & categories of resources available and consumed by: • Projects • Enhancements • Maintenance service • Maintenance break/fix • Maintenance compliance • New activities (non-project).	TBD	TBD
B02.002	Resource Management	Provide resource allocation capability.	TBD	TBD
B02.003	Resource Management	Provide staff/resource crosswalk to CAPPS FIN department ID.	TBD	TBD
B02.004	Resource Management	Have the ability to support state employee, contract labor and 3rd party.	TBD	TBD
B02.005	Resource Management	Have the ability to set configurable permissions by user role.	TBD	TBD
B02.006	Resource Management	Identify resources available by role: • developer • tester •business analyst •project manager •DBA •IG Actuary •IG Administrative Assistant •IG Attorney •IG Investigator •IG Legal Assistant •IG Management •IG Program Specialist •IG Research Specialist.	TBD	TBD
B02.007	Resource Management	Have the ability to model and manage demand of resources.	TBD	TBD
B02.008	Resource Management	Have the ability to support project and non-project time tracking.	TBD	TBD
B02.009	Resource Management	Not used		
B02.010	Resource Management	Have the ability to identify activity-based roles.	TBD	TBD
B02.011	Resource Management	Create an inventory of skill sets inventory within resource management including the level of the skill set.	TBD	TBD
B02.012	Resource Management	Provide ability to forecast project resource costs.	TBD	TBD
B02.013	Resource Management	Provide ability to assign resources by name or role to projects.	TBD	TBD
B02.014	Resource Management	Not used		

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
B02.015	Resource Management	Provide ability to input high-level resource information in order to manage overall capacity.	TBD	TBD
B02.016	Resource Management	Provide ability to forecast resource information across multiple projects.	TBD	TBD
B02.017	Resource Management	Provide ability to record and maintain effective date for employment actions (i.e., hire, transfer, termination).	TBD	TBD
B02.018	Resource Management	Provide ability to record and maintain effective date for department IDs (including retaining the history of department IDs).	TBD	TBD
B02.019	Resource Management	Provide ability to group updates (ex., when department ID changes for an entire group of employees, provide ability to do a group update rather than one employee at a time).	TBD	TBD
B02.020	Resource Management	Not used		
B02.021	Resource Management	Provide exception reporting on un-entered time allocation submission.	TBD	TBD
B02.022	Resource Management	Provide ability to plan capacity, allowing gaps for training, vacation, other non-project work, etc.	TBD	TBD
B02.023	Resource Management	Provide ability to provide additional attributes to project/application (example: charge codes, notes).	TBD	TBD
B02.024	Resource Management	Provide ability to report resources by direct manager.	TBD	TBD
	Business Topic	**Financial & Cost Allocation**		
B03.001	Financial & Cost Allocation	Provide accurate information for cost allocation.	TBD	TBD
B03.002	Financial & Cost Allocation	Comply with all state and federal financial requirements.	TBD	TBD
B03.003	Financial & Cost Allocation	Track project staff (employee) costs.	TBD	TBD
B03.004	Financial & Cost Allocation	Include staff benefits costs.	TBD	TBD
B03.005	Financial & Cost Allocation	Include project staff costs in project.	TBD	TBD
B03.006	Financial & Cost Allocation	Track all contractor costs on projects.	TBD	TBD
B03.007	Financial & Cost Allocation	Provide accurate hours worked information for cost allocation.	TBD	TBD
B03.008	Financial & Cost Allocation	Provide consistent process for establishing SDFC.	TBD	TBD
B03.009	Financial & Cost Allocation	Provide effective date for projects and funding.	TBD	TBD
B03.010	Financial & Cost Allocation	Provide ability to record project attributes.	TBD	TBD
B03.011	Financial & Cost Allocation	Have the ability to configure and/or calculate project costs for reporting to QAT and Feds.	TBD	TBD
B03.012	Financial & Cost Allocation	Have the ability to set up/ configure projected budgets.	TBD	TBD
B03.013	Financial & Cost Allocation	Provide ability to forecast assumed monthly run rate.	TBD	TBD

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
B03.014	Financial & Cost Allocation (TIERS)	Provide ability to select a Client Modernization Program from a drop-down list (yes/no).	TBD	TBD
B03.015	Financial & Cost Allocation	Require SDFC funding code at time of project set-up for projects using time and effort cost allocation.	TBD	TBD
	Business Topic	**Policy & Compliance**		
B04.001	Policy & Compliance	Create policy on time allocation to projects & non-project time.	TBD	TBD
B04.002	Policy & Compliance	Provide controls to ensure all time is allocated.	TBD	TBD
B04.003	Policy & Compliance	Provide control to ensure managerial or project manager approval of time allocation to specific projects.	TBD	TBD
B04.004	Policy & Compliance	Provide access control & consistent means for establishing all projects and related criteria.	TBD	TBD
B04.005	Policy & Compliance	Not used		
B04.006	Policy & Compliance	Anytime not directly associated with one of the OIG areas, use the Administrative Time row. (This includes: A/L, S/L, OIG-IT Trainings, OIG-IT Staff meetings, OIG Conferences, etc.).	TBD	TBD
B04.007	Policy & Compliance	Provide ability to set auto reminders for staff who are delinquent on their time allocation reporting.	TBD	TBD
B04.008	Policy & Compliance	Not used		
B04.009	Policy & Compliance	Not used		
B04.010	Policy & Compliance	Not used		
B04.011	Policy & Compliance	Clean up inventory of department IDs (close old department IDs).	TBD	TBD
B04.012	Policy & Compliance	Clean up inventory of resources (remove resources no longer available).	TBD	TBD
B04.013	Policy & Compliance	Have the ability to support federal time allocation and reporting requirements.	TBD	TBD
B04.014	Policy & Compliance	For all records, the retention period is to 10 years. The data migration should include only those records that fall within the retention period defined.	TBD	TBD
	Business Topic	**Reporting**		
B05.001	Reporting	Provide flexible/usable reports, both ad hoc and canned report.	TBD	TBD
B05.002	Reporting	Have the ability to track/report on time/expense per project.	TBD	TBD
B05.003	Reporting	Have the ability to track/report on time/expense per program.	TBD	TBD
B05.004	Reporting	Have the ability to track/report on time/expense per portfolio.	TBD	TBD
B05.005	Reporting	Have the ability to track/report on time/expense per resource.	TBD	TBD
B05.006	Reporting	Have the ability to track/report on time/expense per IT department/team (department ID).	TBD	TBD

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
B05.007	Reporting	Have the ability to report across a configurable time range, such as state or federal fiscal years.	TBD	TBD
B05.008	Reporting	Have the ability to view breakdowns of planned vs. actual work for employees as well as contractors.	TBD	TBD
B05.009	Reporting	Have the ability to customize reports and share/export them as PDFs, word documents, XML or excel files.	TBD	TBD
B05.010	Reporting	Have the ability to create customizable dashboards to support reporting and decision-making needs, including release management.	TBD	TBD
B05.011	Reporting	Report by individuals a weekly time allocation reflecting all time for the week.	TBD	TBD
B05.012	Reporting	Report actual time charged or needed by role on an adhoc or standard report.	TBD	TBD
B05.013	Reporting	Report actual time charged or needed by type of activity.	TBD	TBD
B05.014	Reporting	Report actual time charged or needed by skill set	TBD	TBD
B05.015	Reporting	Display the current portfolio (via a view or dashboard of the health and status of proposals and/or projects).	TBD	TBD
B05.016	Reporting	Provide ability to roll up and report program information independently of project information.	TBD	TBD
B05.017	Reporting	Provide project level management dashboards.	TBD	TBD
B05.018	Reporting	Provide portfolio high-level time reporting.	TBD	TBD
B05.019	Reporting	Provide portfolio-level management dashboard.	TBD	TBD
B05.020	Reporting	Report activity/costs for multiple months on single report.	TBD	TBD
B05.021	Reporting	Provide ability to compare required work hours to reported hours and generate exception report for un-entered hours by resource.	TBD	TBD
B05.022	Reporting	Provide ability to set up default notifications for staffing profiles and resource pools.	TBD	TBD
B05.023	Reporting	Provide ability to identify projects/applications missing SDFC.	TBD	TBD
B05.024	Reporting	Maintain customization for the custom dashboards that track resource hours and software modifications by a release.	TBD	TBD
	Business Topic	**Scheduling**		
B06.001	Scheduling	Have the ability to configure and/or calculate schedules.	TBD	TBD
B06.002	Scheduling	Have the ability to integrate (bi-directionally) with other third-party software, such Microsoft Project, JIRA, salesforce, project reporting tools.	TBD	TBD
B06.003	Scheduling	Track time to the deliverable in the project - which deliverable did the person do the work toward.	TBD	TBD
B06.004	Scheduling	Create work breakdown structures.	TBD	TBD
B06.005	Scheduling	Provide ability to create work plan templates.	TBD	TBD
	Business Topic	**Demand Management**		

Rqmt ID	Technical or Business Topic	Description (This system will…)	Module(s)	Phase
B07.001	Demand Mgmt.	Allows for standardized, automated project request collection of multiple types (ideas, proposals, work requests, projects, application enhancement, defect fixes, etc.) with corresponding data, content and business rules.	TBD	TBD
B07.002	Demand Mgmt.	Provide proposal creation and management.	TBD	TBD
B07.003	Demand Mgmt.	Provide approval/workflow process management/life cycle.	TBD	TBD
B07.004	Demand Mgmt.	Provide risk analysis and management.	TBD	TBD
B07.005	Demand Mgmt.	Provide what-if scenario planning and analysis.	TBD	TBD
B07.006	Demand Mgmt.	Provide inter-project dependency definition.	TBD	TBD
B07.007	Demand Mgmt.	Risk analysis and management.	TBD	TBD
B07.008	Demand Mgmt.	Provide ability to group projects into programs.	TBD	TBD
B07.009	Demand Mgmt.	Provide ability to group projects into portfolios.	TBD	TBD

Exhibit I-2 - User Story Narratives

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Program	to quickly get my needs to IT	they can get working on them.	TBD	1
			x		Program	to quickly get my needs to IT	I can plan and balance other work.	TBD	TBD
			x		Governance	to track stages of idea through PM framework	we can get to the doing better.	TBD	TBD
			x		Governance	to map pipeline to portfolio roadmaps	we can manage those roadmaps.	TBD	TBD
			x		CIO/CITO	to know when the outcome of a project affects the portfolio	we can minimize negative impact.	TBD	TBD
			x		CIO/CITO or Governance	a methodology and process to absorb change in portfolio	we can minimize risk of overloading the organization.	TBD	TBD
			x		CIO/CITO	to know the status - green, yellow, red	I can "help" with red projects.	TBD	TBD
			x		CIO/CITO	to know all projects over 5 million dollars	I have awareness of all MIRPS.	TBD	TBD
			x		CIO/CITO	to see the pipeline of projects	I can understand our programs' priorities.	TBD	TBD
			x		CIO/CITO	to know the priority of projects	I can make sure folks are focused on the right things.	TBD	TBD
			x		Project Manager	to know as project milestones are reached or not met	I can take corrective measures for delays & report up on them & also report on successes.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Portfolio Manager	to know when resources roll off a project -- when they become available	I can reassign them to work in the queue and better manage my portfolio.	TBD	TBD
			x		Portfolio Manager	to know when next project stages are hit or delayed	I can properly alert management & work with the team towards course correction.	TBD	TBD
			x		Portfolio Manager	to know when a new project is added to the queue & its priority	I can ensure a designated resource is working on the right thing.	TBD	TBD
			x		Applications development director	to know which projects in the queue have the highest priority	I can begin working on resource needs.	TBD	TBD
			x		Applications development director	to be notified of major projects that are in trouble status	I can request correction plans from responsible directors.	TBD	TBD
			x		Portfolio Manager	to see project health of all projects in my portfolio	I can address any issues of projects encountering difficulties.	TBD	TBD
			x		Portfolio Manager	to see any deliverables scheduled to be complete in the next month & information as to whether they will complete on time	I can manage expectations of customers & reassign resources if needed to meet deadline.	TBD	TBD
			x		Portfolio Manager	to see history & forecast of projects for fiscal year	I can manage workload, resources & know when problems are coming up.	TBD	TBD
			x		Portfolio Manager	to see a comparison of all projects showing stage of life cycle the project is in	I can be aware of possible resource shifting needs & when projects can be moved into the work queue.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Project Manager	to see charts & graphs showing actual/budget & warnings to be generated when budget is going to be exceeded (money or hours)	I can manage project budget.	TBD	TBD
			x		Project Manager	to see schedules showing estimated & expended	I know where the budget/schedule stands & can manage expectations.	TBD	TBD
			x		Project Manager	the ability to easily set up Work Breakdown Structure from templates that can be edited	I can establish the staffing need over time & overall schedule.	TBD	TBD
			x		Project Manager	a standardized way to indicate project health -- what makes a project red, yellow, green	Project health is reported in a consistent manner.	TBD	TBD
			x		Applications development director	the ability to see resource capacity across all portfolios	I can reassign resources as priorities change.	TBD	TBD
			x		Applications development director	the ability to prioritize & change priorities on projects	I can adjust effort as required by Commission leadership.	TBD	TBD
			x		Applications development director	the ability to determine above & below line projects	resources are not over allocated & workload is reasonable.	TBD	TBD
			x		Applications development director	to know project health	I am able to address projects in trouble.	TBD	TBD
			x		Project Manager	an easy quick way to escalate help needed to management	I can keep my project on track.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Project Manager	an efficient way to update project status/risk/issues in one place	I can efficiently update a single time.	TBD	TBD
			x		Applications development director	to see budget health for project portfolios -- delta to budget exceptions	I can manage project or portfolio budget exceptions.	TBD	TBD
			x		Applications development director	to see project pipeline including projects in execution as well as backlog	I can manage portfolios of projects.	TBD	TBD
			x		Applications development director	to see resource variances for projects	I can manage portfolios of projects.	TBD	TBD
			x		Portfolio Manager	to create, edit, delete a Work Breakdown Structure	I can track non-project activities in my organization; review resource time expended outside of projects.	TBD	TBD
			x		Portfolio Manager	the ability to assign project teams to approved service requests for my organization	I can staff approved projects.	TBD	TBD
			x		Portfolio Manager	the ability to automatically create projects from approved service requests for my organization	I can track time for approved service requests.	TBD	TBD
			x		Portfolio Manager	to create, edit, delete service requests	I can manage work within my organization.	TBD	TBD
			x		Portfolio Manager	to create, edit, delete requests for IT services from my organization	I can manage the work intake.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Applications development director	to create, edit, delete a Work Breakdown Structure to track "overhead" activities in my organization	I can manage overhead tracking.	TBD	TBD
			x		Applications development director	to assign, reassign, remove projects to portfolios	I can manage project assignments.	TBD	TBD
			x		Applications development director	to create, edit, delete portfolios	I can manage portfolios.	TBD	TBD
			x		Project Manager	to create a project from a list of projects templates	new projects are easily created.	TBD	TBD
			x		Project Manager (contractor services)	to create, edit, delete custom projects	vendor's work breakdown structure activities can be tracked.	TBD	TBD
			x		Project Manager	to track project approved workflow, assignments, including comment history & attached documentation	To maintain information in one repository.	TBD	TBD
			x		Project Manager	to include cost allocation (SDFC, impacts program 'n') in project information	to know funding when setting up a project.	TBD	TBD
			x		Finance (Budget/ Accounting)	front end checks & security roles for all SDFCs added to the PPM system	to ensure data fidelity.	TBD	TBD
			x		CIO/CITO	a standard SDP	we can share with program.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
			x		Governance	on demand status of projects	we can quickly make informed decisions.	TBD	TBD
			x		Governance	a prioritized pipeline & why (business driver)	we know that we are working on the right things.	TBD	TBD
			x		Governance	to know that deliverables are being met	I can measure or assess quality.	TBD	TBD
			x		Portfolio Manager	to review & approve my monthly budget forecast	I can verify available budget.	TBD	TBD
			x		Applications development director	to review & approve monthly budget forecasts	I can verify available budget.	TBD	TBD
				x	Program	a dashboard that shows overall health/problems	we can prioritize work.	TBD	TBD
				x	Governance	an ahead/behind report per project	we can summarize & determine status: --financial --resource --schedule.	TBD	TBD
				x	CIO/CITO	an ahead/behind report per project	we can make resource decisions.	TBD	TBD
				x	CIO/CITO	an overall cross portfolio health dashboard	I can communicate with IT/program concerning health.	TBD	TBD
				x	Governance	a dashboard that shows overall health/problems per portfolio	we can manage in governance steering committee.	TBD	TBD
				x	Governance	a report that shows what strategic initiatives or projects are lined up with	we can communicate what we are working on & what we are working for.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Governance	a report/dashboard that shows alignment with agency strategic plan	we can track against program goals.	TBD	TBD
				x	Governance	a project pipeline dashboard that has schedule/ status/ resources/ stage/state/what is in queue	we can communicate to stakeholders.	TBD	TBD
				x	Program	a report that shows value/outcomes	I can focus decisions toward better.	TBD	TBD
				x	CIO/CITO	to see available resource capacity per portfolio	I can communicate & prioritize work.	TBD	TBD
x				x	CIO/CITO	a report on resources	I can make resource allocation decisions.	TBD	TBD
				x	CIO/CITO	a dashboard for pipeline financials	I can manage financial goodness within each portfolio.	TBD	TBD
				x	CIO/CITO	to see upcoming/ proposed projects and estimated resource needs	we can plan next steps	TBD	TBD
				x	CIO/CITO	to have a dashboard for project pipelines for each portfolio/sub-portfolio	I can see the health of each portfolio	TBD	TBD
				x	CIO/CITO	to see overall project health per portfolio	we can communicate to program how we are doing	TBD	TBD
				x	CIO/CITO	to see a cross portfolio pipeline dashboard	I can see the pipeline (health across all portfolios)	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	QBR preparer	a list of all approved FY key projects by portfolio with ID number, status (red, yellow green, completed, cancelled), status comment (explanation/mitigation)	I can report on QBR and comply with C-050	TBD	TBD
				x	Fed/state reporting coordinator	The QMR for each MIRP to prepopulate budget data	we are consistent, accurate & efficient	TBD	TBD
				x	ITBO	SDFCs to have effective dated rows in case of shifts or changes, and a historical table of SDFCs with definitions	we can provide more accurate reporting without the need to set up new SDFCs.	TBD	TBD
				x	Fed/state reporting coordinator	to document & track QAT decision on frequency of monitoring	we have a record of QAT decisions	TBD	TBD
				x	ITBO & Fed/state reporting coordinator	two views of actuals:1 - SFY on an accrual basis (month of service)2 - FFY on a cash basis (month of payment)	I may provide both fed & state reports	TBD	TBD
				x	Op plan & QBR preparer	to know which HHS strategic priorities a project is related to	I can align the work of the division with the goals of the organization	TBD	TBD
				x	CIO/CITO	standard templates that ensure project level documents & data are standardized (red means red)	I can be assured that the PPM level decisions are based on solid data.	TBD	TBD
				x	CIO/CITO	to map the project pipeline to the portfolio & 5-year roadmaps	I can manage the portfolio & strategic roadmaps	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	CIO/CITO	a list of projects across portfolios that align to a strategy	I can see alignment with program strategies	TBD	TBD
				x	CIO/CITO	to see all projects below line & reason why	so that we can disposition (Exceptional Item-ok staff - maybe not)	TBD	TBD
				x	IT staff	a dashboard of projects that resource has worked on	I can review historical activity	TBD	TBD
				x	ITBO & Fed/state reporting coordinator	to categorize all projects systematically & formalize decisions on whether something is a MIRP	we are consistent & have records & more information visible	TBD	TBD
				x	CIO & Portfolio Director	DIR-TSO-g indicator on cost (calculated by average spent per month $ & time - burndown)	I know if we are headed toward red cost status	TBD	TBD
				x	Dashboard contributor	to know quarterly state reports submitted timely for the quarter	I can report on the CIO dashboard	TBD	TBD
				x	CIO, dashboard preparer & Portfolio Director	a way for PMs to communicate trending status for cost, time, scope, etc.	I can be informed about an upcoming potential status change	TBD	TBD
				x	ITBO	to track if specific SDFC codes/time is direct or informational cost associated to a MIRP/ APD/ Capital project	I may provide better fed/state reporting	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Dashboard contributor	to know quarterly Fed reports submitted timely for the quarter	I can report on the CIO dashboard	TBD	TBD
				x	Preparer of the operational plan	a listing of all approved key projects (new & continuing) for the fiscal year with portfolio & ID number	I can report on operational plan & comply with C-050	TBD	TBD
				x	Finance (Budget/ Accounting)	statistics with definitions of the SDFCs/projects based on verified actuals	we can produce sound cost allocation data	TBD	TBD
				x	Finance / Forecasting	access to project financial cost	projects can be reported with actuals compared to planned costs	TBD	TBD
				x	Finance staffer	to see project informational costs	we can report costs in legislative reports	TBD	TBD
				x	ITBO Forecaster (Partially TIERS as identified in footnote)	to run reports by project/subproject[1]/task & by month	resource costs can be reported	TBD	TBD

[1] HHSC IT does not want to track time at the task level within a WBS. The ability to track time by project task is very critical in current TIERS PPM time reporting configuration. The following types of PPM Projects are used to support time reporting:

- IT General Project
  - Used to track time for "global" IT organization activities across all organizations
  - Tasks include: Training, Career Evaluations, Leave/Holidays
- IT Apps Social Project
  - Used to track standard IT Apps Social organization activities
  - Tasks used to track 14 types of application support activities
  - Tasks used to track 4 types of administrative activities
- TIERS Release Projects (one project created per release)

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	ITBO Forecaster or Finance	details to numbers reported in PMRS status reports	financial information can be reported as needed (e.g., by strategy, capital project, APD)	TBD	TBD
		x		x	ITBO forecast staffer	to know when all staff reporting is complete	monthly cost allocation reports can be generated	TBD	TBD
				x	ITBO forecast staffer	a supervisor validation of time reported	time reported is accurate & reasonable	TBD	TBD
				x	ITBO forecast staffer	a list of staff not yet reported	a reminder can be sent to them automatically	TBD	TBD
				x	ITBO forecast (Partially TIERS as identified in the footnote)	the ability to generate reports or dashboards for hours by project/ subproject/ task[2]	we can facilitate expenditure reporting and/or ETVs	TBD	TBD
				x	Fed/state reporting coordinator or submitter	access to cost information	costs are reported with consistent & accurate information	TBD	TBD
		x		x	ITBO forecast staffer	to have the ability to modify user portfolio with effective dates	user profile history is maintained & allows for multiple cost allocation reports	TBD	TBD

- o Used to track support of each TIERS release
- o Tracks 12 types of release support and software maintenance activities
- TIERS Service Request Projects (one per TIERS sprint)
  - o Used to track sprint activities

[2] Ibid.

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Fed/state coordinator	to know the frequency of reports	I can see when reports are due and status	TBD	TBD
				x	Fed/state coordinator	to know when & what APDs or MIRPs are required	I can prepare submissions timely	TBD	TBD
				x	ITBO forecast staffer	to run a report of hours reported	I can ensure all required hours are reported	TBD	TBD
				x	IT staff	to know when & who is required to report	I can report in system timely	TBD	TBD
				x	Project manager	a report of assigned resources (staff) allocation reflecting time projected for other projects	I can better identify risks when resources are assigned multiple projects	TBD	TBD
				x	Portfolio Director	a dashboard that reflects staff utilization against capacity	I can identify under/over utilized resources & better leverage skills	TBD	TBD
				x	Portfolio Director	to track the health of the budget for my portfolio	I can make necessary adjustments on a regular basis instead of end of year chunk	TBD	TBD
				x	Portfolio Director	a single visual representation of the health of a project	I can determine where more attention is needed at a glance	TBD	TBD
				x	Project manager	to view the overall health of my projects with drill down on reasons for yellow/red status	I can proactively course correct to deliver according to plan	TBD	TBD
				x	Project manager	to track the actual amount spent against project budget	I can make necessary adjustments to ensure ROI	TBD	TBD
				x	Project manager	to track stage-gate start & end dates against the project plan along with %	I can identify deviations early	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	IT staff	a dashboard of my completed time reporting	I can verify accuracy of recorded time	TBD	TBD
				x	Project manager	a dashboard with total hours expended on project by resource	I can verify accuracy of recorded time	TBD	TBD
				x	Project manager	a report of the total hours expended & planned for each Staff Aug resource	I can manage resource effort against PO	TBD	TBD
				x	Project manager	a report of contracted services resource total expended time & actual cost by contract/project	I can verify compliance with time and material work	TBD	TBD
				x	Project manager	a report of contracted services resource time by contract by month	I can verify compliance with contract resource plan	TBD	TBD
				x	Project manager	a report of total hours reported by resource by project	I can verify accuracy of recorded time	TBD	TBD
				x	Project manager	a dashboard of time reporting status by resource	I can verify timeliness of time reporting submitted	TBD	TBD
				x	Project manager	a report of individual time reporting by individual	I can verify accuracy of recorded time	TBD	TBD
				x	Portfolio manager	a dashboard that provides real-time status agile dashboard	to continue my current real-time view of sprint status	TBD	TBD
				x	Portfolio manager (TIERS)	a dashboard that provides all capabilities of current TIERS agile dashboard	to continue my current real-time view of sprint status	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Portfolio manager	a dashboard of all projects planned to be executed in the next month, quarter	I can allocate project to available teams	TBD	TBD
				x	Portfolio manager	a dashboard by month, quarter of projects assigned to team	I can identify available teams	TBD	TBD
				x	Portfolio manager	a report of resources by Department ID and company	I can track accuracy of resource data in PPM	TBD	TBD
				x	Portfolio manager	a dashboard of in-process projects with drilldown to assigned resources	I can reallocate resource to meet emergency request	TBD	TBD
				x	Applications development director	a dashboard of portfolio initiative forecaster - labor by initiative	I can track total forecasted resource commitment	TBD	TBD
				x	Applications development director	a dashboard of total expended vs. obligated budget by forecast item	I can assess budget status	TBD	TBD
				x	Applications development director	a report on non-project time allocation	I can access percent of resource time on overhead work	TBD	TBD
				x	Applications development director	a report on resource time by Staff, Staff Aug, Contracts Services	I can assess percent of labor provided by category	TBD	TBD
				x	Applications development director	a report on total actual resource time on all projects	I can access actual labor allocations	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Applications development director	a dashboard to see the pipeline of approved and/or requested projects	I can effectively plan resources and projects	TBD	TBD
				x	Applications development director	a dashboard showing resource cost spent on projects to date	I can manage my budget	TBD	TBD
				x	Applications development director	a report showing inventory of skills & resource names/quantity by skill	I can assign & forecast resources to work	TBD	TBD
				x	Applications development director	a dashboard of the skills of resources in my organization	I can plan resource allocation for current & future work	TBD	TBD
				x	Applications development director	a dashboard of project status & key risks/issues	I can more effectively provide oversight to portfolio of projects	TBD	TBD
				x	Applications development director	a dashboard to see how much organization time spent on categories of work such as meetings, development, project work, maintenance, testing, etc.	I can manage resources efficiently	TBD	TBD
				x	Portfolio manager	a dashboard showing list & status of all my projects	I can manage my portfolio of projects	TBD	TBD
				x	Portfolio manager	a report showing how many available vs. utilized hours my team has by person and/or skill	I can effectively manage my resources	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Portfolio manager	a report showing time spent by person/ by item in categories of work - meetings, development, test, analysis, projects, break-fix, etc.	I can manage my team	TBD	TBD
				x	Project manager	a report showing time spent by project resources in non-project related work	I can manage resource availability issues	TBD	TBD
				x	Project manager	a report to see actual hours worked vs. planned or allocated hours by resources & by type of work	I can identify & manage resource availability	TBD	TBD
				x	Project manager	a reporting system to show the status/key risks/ issues/help needed for my project	I have efficient way to ensure management visibility of my project & help needed	TBD	TBD
				x	Project manager	a report to show all resources, hours and cost spent on my project by fiscal month	I can generate required QAT reports & track project costs	TBD	TBD
				x	Applications development director	a dashboard view of current place in schedule for each project compared to estimated time to complete	I can see if projects are running behind	TBD	TBD
				x	Applications development director	a dashboard view of resources	I can see availability of resources for proposed work	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Applications development director	a dashboard view of remaining time/budget to estimate to complete	I can see if projects are on schedule & in budget	TBD	TBD
				x	Applications development director	a report tracking resources worked for individual projects & break-fix	I can identify why projects may be delayed (i.e., diverted resources)	TBD	TBD
				x	Applications development director	a report showing tracking of work done on production systems	I can know how much time is available to be assigned to projects	TBD	TBD
				x	Portfolio manager	a dashboard of all projects time expended	I can see remaining time planned vs. estimate to complete	TBD	TBD
				x	Portfolio manager	a dashboard view of all statuses by health indicators	I can determine projects in need of remediation/ assistance	TBD	TBD
				x	Portfolio manager	a view of all resources available by skills	I can determine if proposed projects can be started	TBD	TBD
				x	Project manager	a single system for all project related reporting & management	I can more easily complete my reporting & can better manage my project	TBD	TBD
				x	Project manager	a way to obtain staff information (phone, location, email, pay rate) for staff & contractors	I can contact/find individuals & better budget resources	TBD	TBD
				x	Project manager	to see available resources (staff, staff augmentation & contracted)	I can determine how to schedule project work	TBD	TBD
				x	Project manager	to identify work necessary to reach a milestone/deliverable	I can have interim acceptance/sign off for project throughout life of the project	TBD	TBD
				x	Project manager	estimated rates assigned to each skill set	I can create better project cost estimates	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
				x	Project manager	monthly reporting that shows actual cost of time expended (staff & contractors)	I can accurately report monthly & QAT reporting	TBD	TBD
				x	Project manager	a dashboard that shows status of project schedule actual to planned	I can see if project is on schedule or running behind	TBD	TBD
				x	IT staff	a list of projects to choose from	I can record my time	TBD	TBD
x	x	x			CIO/CITO	to compare resources consumed vs allocated - am I on target?	we can ensure that we are on target	TBD	TBD
x	x	x			CIO/CITO	to ensure quality/measure quality within portfolio	we can communicate confidence level of accurate reporting vs execution	TBD	TBD
x	x	x			CIO/CITO	to categorize resources (FTEs vs staffing)	we can properly manage long term resources	TBD	TBD
x	x	x			CIO/CITO	a process to manage FTEs vs contractors per portfolio	we can manage resources	TBD	TBD
x	x	x			CIO/CITO	to know where there are skill sets outside of IT & outside portfolio	we can leverage if necessary	TBD	TBD
x	x	x			CIO/CITO	to understand resource capacity overall (beyond those earmarked for projects)	we can mitigate issues.	TBD	TBD
x	x	x			CIO/CITO	to manage cost risk within portfolio	within a funding strategy, we can move/manage resources	TBD	TBD
x	x	x			Governance	to compare what we estimated vs actuals	we can refine estimation process	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x	x	x			Governance	to manage governance: --charters --meeting schedule --meeting agendas --communications	we can drive to making decisions	TBD	TBD
x	x	x			Governance	to be able to do what if scenarios for resource, time and cost	we can prioritize future efforts	TBD	TBD
x	x	x			Governance	PPM level RAID	we can track & record decisions & assumptions for portfolio	TBD	TBD
x	x	x			Governance	a methodology to score resource, time considerations, cost & risk	we can make decisions	TBD	TBD
x	x	x			CIO/CITO	a process to id & score risk	we can determine & manage mitigation strategies	TBD	TBD
x	x	x			Program	a process to id & score risk	we can prioritize	TBD	TBD
x	x	x			CIO/CITO	a process to manage budget across portfolio	we can make decisions regarding resources	TBD	TBD
x	x	x			Governance	to show how much type of each resource (FTEs vs contractors) are working on projects per portfolio	we can communicate and estimate how long to staff.	TBD	TBD
x	x	x			CIO/CITO & Governance	a process to allocate & manage resources per portfolio: --time --skills --approved --source resource --capacity --mitigate	we can manage resources	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x	x	x			Governance	to see ROI/utilization of resources	I can show program/stakeholders to explain project outcomes	TBD	TBD
x	x	x			Governance	to show how much time is spent on intake process	we can estimate cost ($) of estimating	TBD	TBD
x	x	x			CIO/CITO	to know where I have a shortage of resources	We can determine next steps	TBD	TBD
x	x	x			CIO/CITO & Governance	a high-level breakout of work categories by portfolio (maintenance-project)	we can discuss capacity & constraints	TBD	TBD
x	x	x			CIO/CITO	to see cost categories (where funded) across portfolios	we can see color of $ vs work done	TBD	TBD
x	x	x			Program	to know what program resources will be needed to complete a project & when	we can allocate resources	TBD	TBD
x	x	x			Portfolio Manager	a project estimating ability to determine cost, effort, time	I can decide if able to start a project	TBD	TBD
x	x	x			Portfolio Manager	a method to prioritize projects	I can manage pipeline & know when to start a project	TBD	TBD
x	x	x			Portfolio Manager	to see all resources by skill & funding	I can assign to projects without affecting budget	TBD	TBD
x	x	x			Applications development director	to know resources (staff & contractor) by skill	I can assign to projects	TBD	TBD
x	x	x			Applications development director	to verify people are assigned to correct projects, break/fix	I can ensure work is in correct & expected area	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x	x	x			Project manager	to see my budget spent, both actual & projected	I can anticipate shortages & take needed action	TBD	TBD
x	x	x			Portfolio Manager	to inventory team member skill sets	I can identify gaps and plan for training/augmentation	TBD	TBD
x	x				Project manager	to know how much of a resource's time is allocated to my project	I can budget their time with respect to other workload	TBD	TBD
x	x				Applications development director	staff to record to projects or break/fix applications	I can tell where effort is being expended	TBD	TBD
x	x				Applications development director	to see individual's work rate compared to estimated rate	I can see if tasks & deliverables are on time	TBD	TBD
x	x				IT staff	to know when my time entered is short or has an error	I can correct entries in a timely manner while my time spent is fresh in my mind	TBD	TBD
x	x				Portfolio Manager	to have staff track time by project/maintenance/break fix	I can identify potential issues with quality/aging apps/etc.	TBD	TBD
x	x				Applications development director	to associate an experience level with individuals & skills	I can appropriately staff my organization & plan for future needs	TBD	TBD
	x				IT staff	a way to easily & quickly enter time for activities I work on	time tracking is not overly cumbersome	TBD	TBD
	x				IT staff	to record my time in the minimum number of lines possible	I can do real work	TBD	TBD
	x				Project manager	the ability to see what non-project work project resources are working on	I can identify and escalate resource availability issues	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
	x				Project manager	to see actual vs planned time for a project	I can improve project task estimations in the future	TBD	TBD
	x				Project manager	a method for project resources to track time against projects on a daily basis	I can report time/cost spent on my projects	TBD	TBD
	x				Applications portfolio director	to know departments & funding sources for all resources -- want to know where I can move resources between departments/ projects & what the budget implications are	I can move resources between projects	TBD	TBD
	x				Applications development director	to know where my team is spending time -- type of work	I can manage my resources	TBD	TBD
	x				IT staff	to search my historical time reporting for specific items	I can correct errors	TBD	TBD
	x				IT staff	to receive notification reminders that my time reporting is due	I can be current on my time reporting	TBD	TBD
	x				IT staff	to correct entries on historical time reporting	I can correct errors	TBD	TBD
	x				IT staff	to easily identify the project item associated with my activity for entry on time reporting	I can easily complete my time reporting	TBD	TBD
	x				IT staff	to create, edit, copy, cancel & submit my time reporting	I can easily create my time reporting	TBD	TBD
	x				Applications development director	to know how much time is spent on administrative tasks (non-project/ non-maintenance)	I can better understand actual capacity of teams	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
	x				Project manager	to review & approve staff augmentation time reporting	duplicate time entry is avoided	TBD	TBD
	x				Project manager	to review & approve time reporting for my assigned resources	verify time reporting accuracy	TBD	TBD
	x				Portfolio Manager	to manually override time reporting entries for my organization as needed	I can cover for resource absence	TBD	TBD
	x				Portfolio Manager	to serve as a proxy time reporting approver for my direct reports	I can cover for out of office staff	TBD	TBD
	x				Project manager	to receive notification of un-submitted time reporting	I can cover for out of office staff	TBD	TBD
	x				Applications development director	to serve as a proxy for my direct reports	I can cover absences & transfers	TBD	TBD
	x				Applications development director	the ability to review & approve the time reporting policies for my organization (policy = time reporting period, max time per day, auto-approve …)	I can ensure consistency as needed	TBD	TBD
x					Applications development director	to know how much time is spent on admin/overhead (meetings, time off, training)	I can create improvement plans & better manage resources	TBD	TBD
x					Applications development director	to know what resources are available & when	I know when projects can start	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x					Applications development director	to see what future staffing needs are for projects in the pipeline	I can plan resources	TBD	TBD
x					Applications development director	to know what all resources in my organization are working on & what it costs	I can make roadmaps for applications	TBD	TBD
x					Applications development director	to see resource & skill gaps to accomplish project pipeline	I can create staffing plans	TBD	TBD
x					IT staff	to easily obtain lines for additional projects for time reporting to record time	I am more productive	TBD	TBD
x					IT staff	time reporting to easily appear when needed with no work on my part	I may expend minimum time on time sheets and more on work	TBD	TBD
x					IT staff	my manager to enter time for me when I'm sick or out	I don't have to come to work when I'm sick -- stay home	TBD	TBD
x					Project manager	costs & hours recorded by contractor	I can verify invoices received	TBD	TBD
x					Project manager	to see all available resources	I can assign to projects	TBD	TBD
x					Project manager	to see all attributes for each resource (location, email, phone, cost, skill)	I can find people for work/ emergencies/ cross covering a task in case of gaps in staffing	TBD	TBD
x					Project manager	to approve time reporting for staff & contractors	I can verify accuracy of time entry	TBD	TBD
x					Project manager	the ability to enter/change time for employees	I can correct incorrect entries	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x					Project manager	to see all hours budgeted & expended by project or individual	I can do the required reporting & identify project health	TBD	TBD
x					Project manager	to record all resource costs (stuff in addition to people)	I can create correct cost reporting & cost estimating for my project	TBD	TBD
x					Applications development director	to adjust workload of resources due to addition/ deletion of staff or contractors	the overall schedule can be adjusted for different staffing levels	TBD	TBD
x					Applications development director	to see the amount of resources by skill level	I can determine shortages in a resources' level of staffing	TBD	TBD
x					IT staff	to be able to update my profile when new skills are gained	I get opportunities to utilize my new skills and grow them	TBD	TBD
x					Project manager	to see when a resource is unavailable due to leave	I can appropriately load my project plan	TBD	TBD
x					Project manager	to know secondary skill sets for project team	I can leverage those to mitigate risks caused by other resource shortages	TBD	TBD
x					Portfolio Manager	to identify staff available by skill set	I can staff upcoming projects appropriately	TBD	TBD
x					Applications development director	to associate a rate with a resource	I can determine average cost across the organization for skill sets	TBD	TBD
x					Applications development director	to inventory skills by team member	I can allocate resources appropriately & augment the teams with needed skills & identify gaps	TBD	TBD
x					Project manager	to assign & remove resources to projects or project teams	I can insure correct team assignment	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x					Project manager	to add, edit, delete skills for my resources	verify skill accuracy	TBD	TBD
x					Portfolio Manager	to on-board, transfer, exit my resources	I can manage my available resources	TBD	TBD
x					Applications development director	to review & approve changes to staff & staff augmentation positions in my organization	I can verify available positions	TBD	TBD
x					IT staff	to view my resource information (skills, department, time approver …)	I can verify my information	TBD	TBD
x		x			Applications development director	to know which people/skills are funded by what Dept. ID	I can move needed resources between teams without negatively impacting budget	TBD	TBD
		x		x	Project manager	to create time allocation reports by department or project	I can verify allocation	TBD	TBD
		x			Portfolio Manager	to view my actual cost allocation (GR, Fed, Cap, non-Cap) against forecast for my budget	I can identify potential shortfalls	TBD	TBD
				x	Federal state coordinator	project status reporting on MIRPs to prepopulate into the QMR & approval by management	there is one source of truth. We are consistent & accurate.	TBD	TBD
				x	Governance	a report that shows stage management (artifacts, static testing, go/no go/communication/tracker/ validation/post go/support	we can communicate to stakeholders.	TBD	TBD

Story Narrative					As a	I want	So that	Module(s)	Phase
Resource Mgmt.	Time Mgmt.	Cost Allocation	Project & Portfolio Mgmt.	Reporting & Dashboards					
x	x	x	x		Program	to ensure time allocation to appropriate fund source	we can support federal time allocation and reporting requirements	TBD	TBD

Exhibit I-3: Glossary

Term	Definition
A/L	Annual leave
APD	Advance Planning Document
APPS	Application
Aug	Augmentation
CAPPS	Centralized Accounting and Payroll/Personnel System
Cap	Capital
C-050	Circular C-050, HHS Operational Plans and Quarterly Business Reports
CIO	Chief Information Officer
CITO	Chief Information Technology Officer
DBA	Data Base Administrator
DIR	Department of Information Resources
DUA	Data Use Agreement
ETV	Expenditure transfer voucher
Fed	Federal
FIN	Finance
FTE	Full time equivalent
FY	Fiscal Year
GR	General revenue
HHS	Health & Human Services
HHSC	Health & Human Services Commission
HP	Hewlett Packard
HPE	Hewlett Packard Enterprise
HSP	HUB subcontracting plan
HUB	Historically under-utilized business
ID	Identification
IT	Information Technology
ITBO	Information Technology Business Operations
JIRA	A proprietary issue-tracking product, developed by Atlassian. It provides bug tracking, issue tracking, and project management functions.
MIRP	Major information resource project
MS	Microsoft
Non-CAP	Non-capital
OIG	Office of the Inspector General
PMRS	Project Management Reporting System
PPM	Project & Portfolio Management
PO	Purchase order
QAT	Quality Assurance Team
QBR	Quarterly Business Report
QMR	Quarterly Monitoring Report

Term	Definition
RAID	Risk, Action, Issues, Decision/Dependencies
RoD	Remedy on Demand
ROI	Return on investment
SDFC	System Designator Funding Code
SDP	Service Delivery Plan - A snapshot of IT activity for a period of time
SFY	State fiscal year
S/L	Sick leave
SPI	Schedule Performance Index - a measure of schedule efficiency as a ratio of earned vs planned value
SWOT	Strengths, Weaknesses, Opportunities, Threats
TIERS	Texas Integrated Eligibility Redesign System
UTCs	Uniform Terms and Conditions

Exhibit I-4: HHS IT Project Tracking, Time Effort Reporting & Cost Allocation Process

1. Purpose 176
2. Scope 176
3. Roles 177
4. Flowcharts and Description 178
5. Metrics 190
6. Related Forms and Documents 190
7. Database and System Applications 191
8. Revision History 192
9. Appendix A. Acronyms 193

1 Purpose

This process establishes guidelines for Health and Human Services (HHS) Information Technology (IT) division projects with planned costs greater than or equal to $100,000. This process explains how these projects are started and ended in the Fiscal Year Plan and the HHS Project Management and Repository System (PMRS). This process also explains the requirements for how people who work on IT projects report time effort into the appropriate time effort reporting system, and how cost is allocated for time effort on a cost allocation.

This process addresses Department of Information Resources (DIR) Project Financial Lifecycle Guide[3] requirements, and Governmental Accounting Standards Board requirements.[4] This process ensures that:

- Requirements in Circular-010: HHS Project Management Policy for IT are met.
- Project-related time is reported in the appropriate time effort reporting system and can be tracked against project budgets.
- Project managers can use time reported in the appropriate system for project reporting.
- Project costs are accurately allocated to the correct funding sources.

Different time effort reporting systems will be used until the HHS IT division completes its project to move all HHS employees to one reporting system:

- Project and Portfolio Management (PPM)
- Salesforce
- BASS
- Dovico

How tasks are operationalized in the following processes may vary based on whether the project has an associated cost allocation factor and which time effort reporting system the project is entered into. Variations includes who serves as the time effort reporting system administrator, whether the project resource reports all time worked or only project-related time, and whether the project is entered into PMRS or not.

2 Scope

This process applies only to HHS projects that have planned costs greater than or equal to $100,000. Processes for adding projects to the Salesforce, BASS, or Dovico time effort reporting systems are out of scope for this document.

[3] See page 13. Requires a standard project budget tracking tool and methodology to ensure consistency and reporting integrity in all project budgets.

[4] See Statement 51: Accounting and Financial Reporting for Intangible Assets.

3 Roles

The following table describes roles and responsibilities associated with this process.

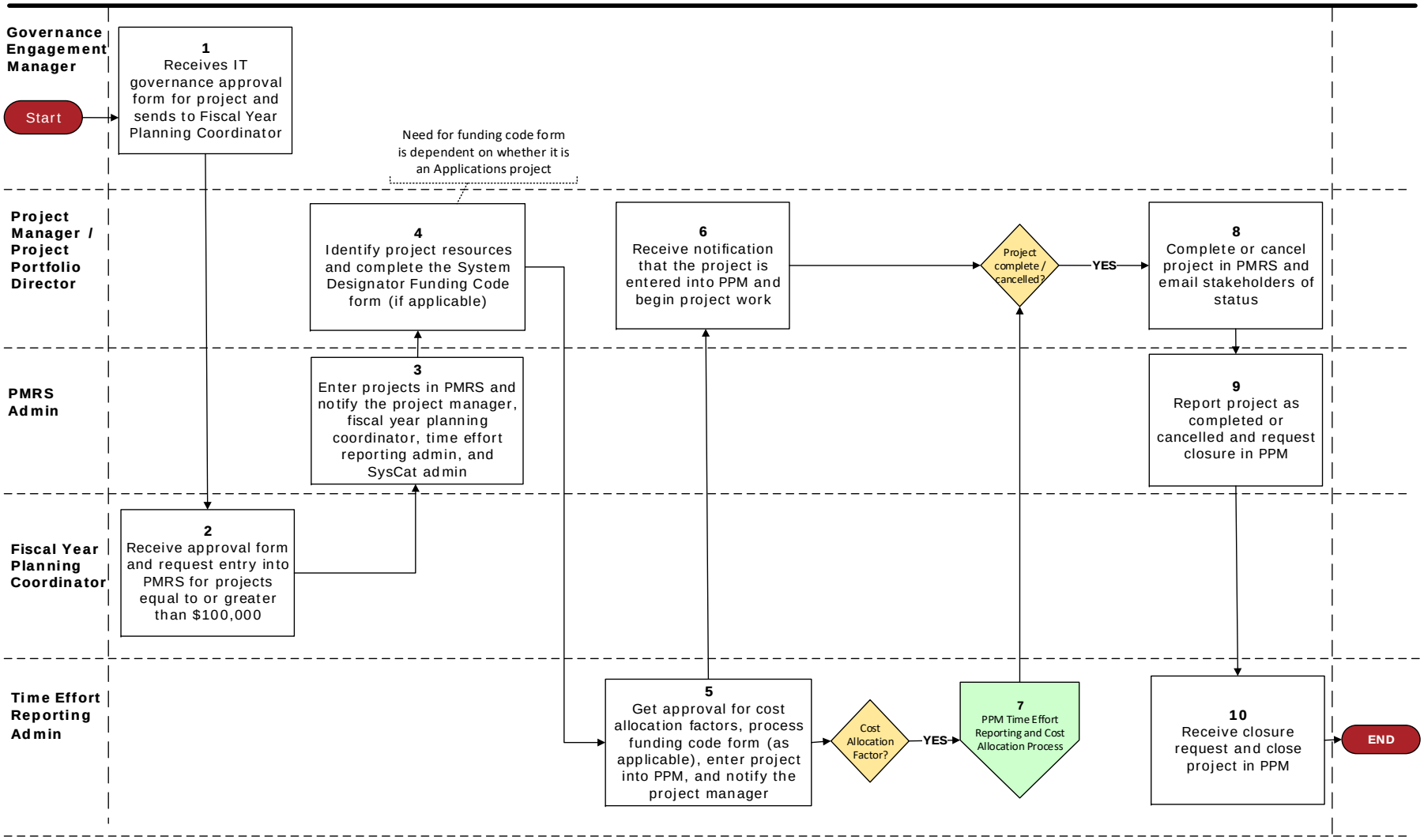
Role	Responsibilities
Cost Allocation	Area of Financial Services that reviews time effort reporting data entered into PPM and Dovico, verifies cost allocation data, and approves the time effort reporting data being submitted into the Fund Accounting Cost Allocation Process.
Fiscal Year Planning Coordinator	Collaborates with the governance engagement manager after projects are approved through the IT governance process, and requests that projects greater than or equal to $100,000 be added to PMRS.
Fund Accounting	Area of Financial Services that receives time effort reporting data via report or HHS IT Statistics System (HISS), verifies percentages for cost allocation, and balances accounting entries in Centralized Accounting and Payroll/Personnel System (CAPPS) Financials.
Governance Engagement Manager	Receives approval form for IT projects that have been approved through the IT governance process and sends approval to fiscal year planning coordinator.
PMRS Administrator	Enters projects greater than or equal to $100,000 into PMRS and notifies the appropriate individuals, tracks completed and cancelled projects, and requests project closure in PPM.
Project Manager	Receives notification when IT projects are entered into PMRS, completes applicable funding code forms, completes or cancels projects in PMRS, and may verify project resource time sheets for certain time effort reporting systems and processes. The project portfolio director may perform some tasks associated with this role if a project manager has not yet been assigned.
Project Portfolio Director	Performs tasks associated with the project manager role if a project manager has not yet been assigned.
Project Resource	Enters time effort into the appropriate time effort reporting system.
Time Effort Reporting Administrator	Processes appropriate funding code forms for applications projects, enters projects into the appropriate time effort reporting systems, and enters time effort reporting data into HISS or submits time effort reporting reports for cost allocation purposes.
Supervisor	May verify project resource time sheets for certain time effort reporting systems and processes.

4 Flowchart and Description

The flowcharts below are a graphical representation of the processes.

4.1 Flowchart Overview – Begin and End Project Process

Only IT projects greater than or equal to $100,000 that are entered into PPM are in scope for this process. The IT Business Operations (ITBO) time effort reporting administrator performs all tasks associated with the time effort reporting administrator in this process.

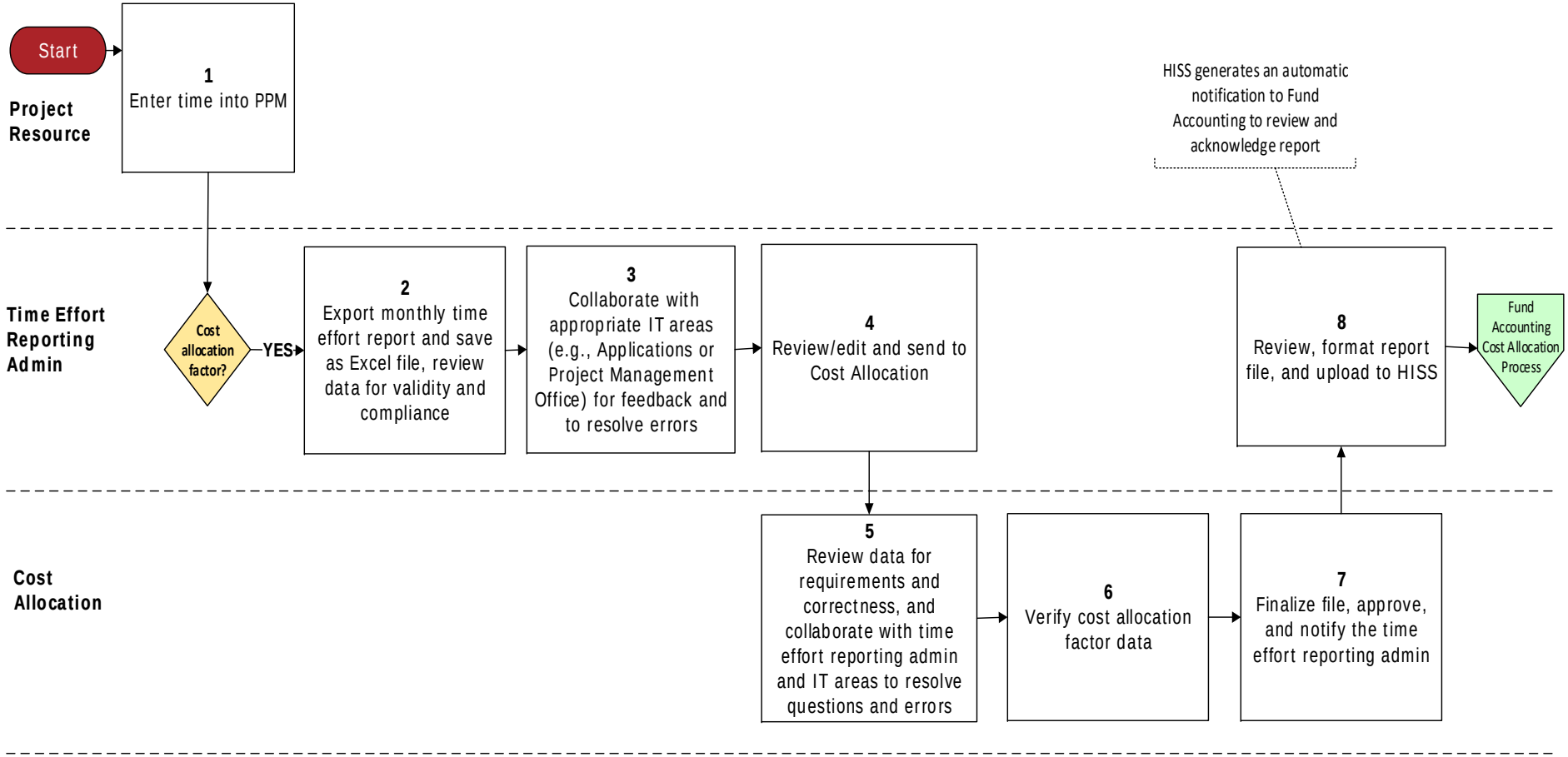

Governance Engagement Manager
Start
1
Receives IT governance approval form for project and sends to Fiscal Year Planning Coordinator
Need for funding code form is dependent on whether it is an Applications project
Project Manager / Project Portfolio Director
4
Identify project resources and complete the System Designator Funding Code form (if applicable)
6
Receive notification that the project is entered into PPM and begin project work
Project complete / cancelled?
YES
8
Complete or cancel project in PMRS and email stakeholders of status
PMRS Admin
3
Enter projects in PMRS and notify the project manager, fiscal year planning coordinator, time effort reporting admin, and SysCat admin
9
Report project as completed or cancelled and request closure in PPM
Fiscal Year Planning Coordinator
2
Receive approval form and request entry into PMRS for projects equal to or greater than $100,000
Time Effort Reporting Admin
5
Get approval for cost allocation factors, process funding code form (as applicable), enter project into PPM, and notify the project manager
Cost Allocation Factor?
YES
7
PPM Time Effort Reporting and Cost Allocation Process
10
Receive closure request and close project in PPM
END

Description – Begin and End Project Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Governance Engagement Manager	1	Receives IT governance process approval for the project and sends approval form to the fiscal year planning coordinator.
Fiscal Year Planning Coordinator	2	Receives the project approval form and requests for the PMRS administrator to enter projects greater than or equal to $100,000 into PMRS.
PMRS Administrator	3	Enters projects into PMRS as requested by the fiscal year planning coordinator. Notifies the project manager / project portfolio director, fiscal year planning coordinator, time reporting admin, and SysCat administrator and provides appropriate guides.
Project Manager / Project Portfolio Director	4	Identifies project resources. If the project is an Applications project, completes the appropriate System Designator Funding Code form. There are two versions of the form. One is for Texas Integrated Eligibility and Redesign System (TIERS) projects and the other is for non-TIERS projects.
Time Effort Reporting Administrator	5	Gets approval for any cost allocation factor. If applicable, ensures the correct funding code form was completed and processes the form. Then, enters the project into PPM. When the project is entered into PPM, notifies the project manager/project portfolio director.
Project Manager / Project Portfolio Director	6	Receives notification from the time effort reporting administrator that the project has been entered into PPM. Begins project work.
Time Effort Reporting Administrator	7	If the project is on a cost allocation factor, follows the PPM Time Effort Reporting and Cost Allocation Process.
Project Manager / Project Portfolio Director	8	When the project is completed or cancelled, completes or cancels the project in PMRS and emails the business stakeholders the status.
PMRS Administrator	9	Reports the project as completed or cancelled and requests closure in PPM.
Time Effort Reporting Administrator	10	Receives closure request from the PMRS admin and closes the project in PPM.

4.2 Flowchart Overview – PPM Time Effort Reporting and Cost Allocation Process

Only IT projects greater than or equal to $100,000 that are entered into PPM are in scope for this process. This process ensures that project resources report their time effort, and that project costs can be accurately allocated to funding sources. The ITBO time effort reporting administrator performs all tasks associated with the time effort reporting administrator in this process.

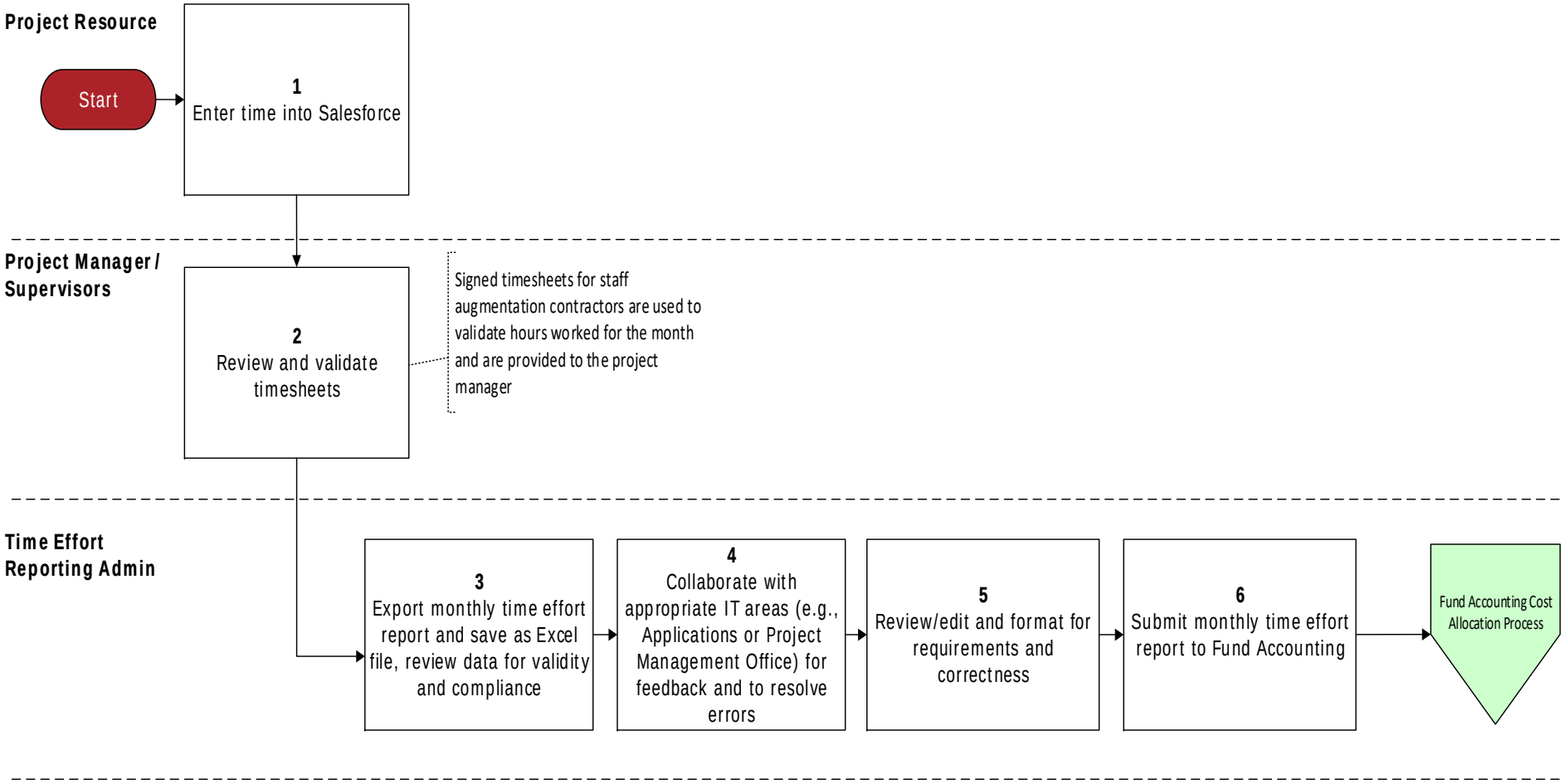


Description – PPM Time Effort Reporting and Cost Allocation Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Project Resource	1	Enters time into PPM using the appropriate project / task.
Time Effort Reporting Administrator	2	Determines if the project is on a cost allocation factor. If it is: • Exports the monthly time entered into the system in the cost allocation factor and saves as an Excel file. • Reviews the data for validity and reporting compliance.
Time Effort Reporting Administrator	3	Collaborates with the appropriate IT areas to get feedback. Examples of IT areas are the Project Management Office and Applications.
Time Effort Reporting Administrator	4	Reviews/edits the data and sends to Cost Allocation.
Cost Allocation	5	Reviews/edits the data for requirements and correctness. Collaborates with the time effort reporting administrator and appropriate IT areas to resolve errors and questions, or to get additional information.
Cost Allocation	6	Verifies cost allocation factor data.
Cost Allocation	7	Finalizes the file, approves, and notifies the time effort reporting administrator.
Time Effort Reporting Administrator	8	Reviews and formats the report file, and uploads it into HISS. HISS generates an automatic notification to Fund Accounting to review and acknowledge the report. This begins the Fund Accounting Cost Allocation Process.

4.3 Flowchart Overview – Salesforce Time Effort Reporting and Cost Allocation Process

Only IT projects greater than or equal to $100,000 that are entered into Salesforce are in scope for this process. This process ensures that project resources report their time effort, and that project costs can be accurately allocated to funding sources. The ITBO time effort reporting administrator performs all tasks associated with the time effort reporting administrator in this process.

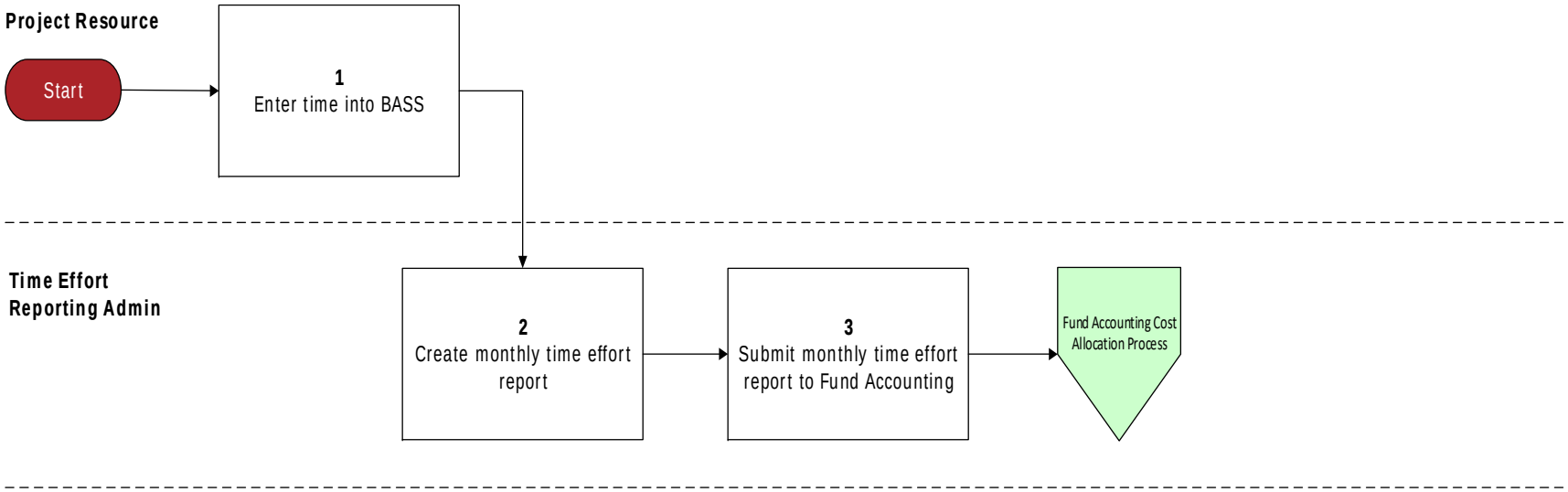


Description – Salesforce Time Effort Reporting and Cost Allocation Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Project Resource	1	Enters time into the system using the appropriate project/task.
Project Manager/ Supervisors	2	Review and validate time effort entered by project resources. Signed timesheets for staff augmentation contractors are used to validate hours worked for the month and are provided to the project manager or supervisor for invoice payments.
Time Effort Reporting Administrator	3	***Exports the monthly time entered into the system in the cost allocation factor and saves as an Excel file.*** ***Reviews the data for validity and reporting compliance.***
Time Effort Reporting Administrator	4	Collaborates with the appropriate IT areas to get feedback. Examples of IT areas are the Project Management Office and Applications.
Time Effort Reporting Administrator	5	Reviews/edits the data for requirements and correctness.
Time Effort Reporting Administrator	6	Submits monthly time effort report to Fund Accounting to begin the Fund Accounting Cost Allocation Process.

4.4 Flowchart Overview – BASS Time Effort Reporting and Cost Allocation Process

Only IT projects greater than or equal to $100,000 that are entered into BASS are in scope for this process. This process ensures that project resources report their time effort, and that project costs can be accurately allocated to funding sources. The appropriate Office of Inspector General (OIG) time effort reporting administrator performs all tasks associated with the time effort reporting administrator in this process.

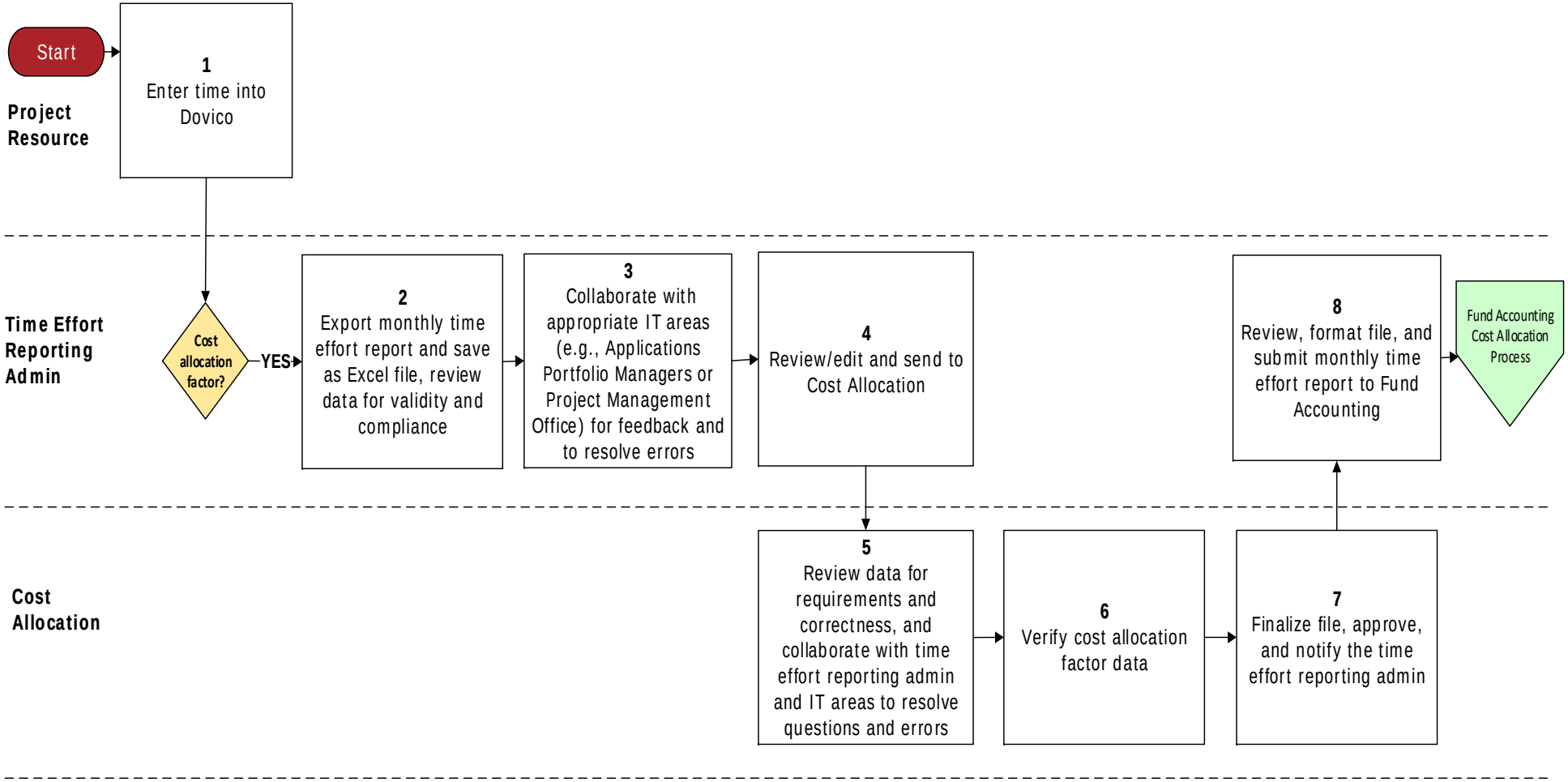


Description – BASS Time Effort Reporting and Cost Allocation Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Project Resource	1	Enters time into BASS using the appropriate project/task.
Time Effort Reporting Administrator	2	Creates the monthly time effort report.
Time Effort Reporting Administrator	3	Submits the monthly time effort report to Fund Accounting to begin the Fund Accounting Cost Allocation Process.

4.5Flowchart Overview – Dovico Time Effort Reporting and Cost Allocation Process

Only IT projects greater than or equal to $100,000 that are entered into Dovico are in scope for this process. This process ensures that project resources report their time effort, and that project costs can be accurately allocated to funding sources. The ITBO time effort reporting administrator performs all tasks associated with the time effort reporting administrator in this process.

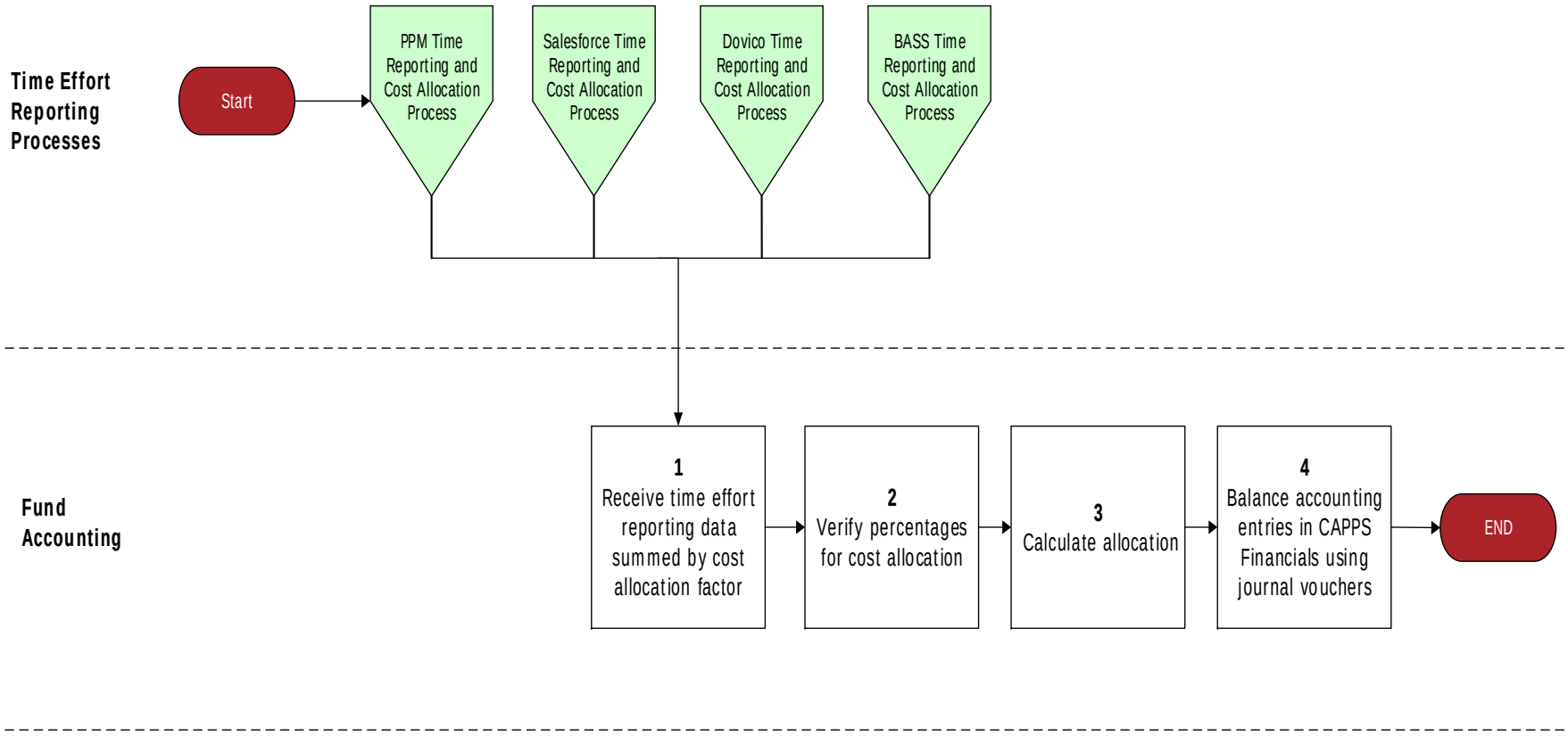


Description – Dovico Time Effort Reporting and Cost Allocation Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Project Resource	1	Enters time into Dovico using the appropriate project/task.
Time Effort Reporting Administrator	2	Determines if the project is on a cost allocation factor. If it is: • Exports the monthly time entered into the system in the cost allocation factor and saves as an Excel file. • Reviews the data for validity and reporting compliance.
Time Effort Reporting Administrator	3	Collaborates with the appropriate IT areas to get feedback. Examples of IT areas are the Project Management Office and Applications.
Time Effort Reporting Administrator	4	Reviews/edits the data and sends to Cost Allocation.
Cost Allocation	5	Reviews/edits the data for requirements and correctness. Collaborates with the time effort reporting administrator and appropriate IT areas to resolve errors and questions, or to get additional information.
Cost Allocation	6	Verifies cost allocation factor data.
Cost Allocation	7	Finalizes the file, approves, and notifies the time effort reporting administrator.
Time Effort Reporting Administrator	8	Reviews, formats file, and submits monthly time effort report to Fund Accounting to begin the Fund Accounting Cost Allocation Process.

4.6 Flowchart Overview – Fund Accounting Cost Allocation Process

Only time effort that is reported and is on a cost allocation factor is in scope for this process. This process begins when time effort on a cost allocation factor that is reported into one of the time effort reporting systems is submitted to Fund Accounting for cost allocation either through HISS, or as a report. This process ensures that project costs are accurately allocated to funding sources.



Description – Fund Accounting Time Effort Cost Allocation Process
The following table describes roles and tasks associated with this process.

Role	Process Flow Number	Task
Fund Accounting	1	Receives time effort reporting data summed by cost allocation factor.
Fund Accounting	2	Verifies percentages for cost allocation.
Fund Accounting	3	Calculates allocation.
Fund Accounting	4	Balances accounting entries in CAPPS Financials using journal vouchers.

5 Metrics

Metrics are not reported for this process.

6 Related Forms and Documents

6.1 Forms

The following forms are used in this process.

Form	Description	User Role	Location
Non-TIERS System Designator Funding Code Request Form	Used to request a non-TIERS IT project funding code for PPM.	Project managers	Time and Cost Allocation SharePoint
TIERS System Designator Funding Code Request Form	Used to request a TIERS IT project funding code for PPM.	Project managers	Time and Cost Allocation SharePoint

6.2 Reference Documents

The following reference documents are used in this process.

Document	Description	User Role	Location
Circular-010: HHS Project Management Policy for Information Technology	Establishes HHS IT project management requirements.	All roles	HHS Connection Policies and Rules Repository
Fiscal Year Planning Guide	Identifies the upcoming fiscal year's project initiatives.	Fiscal year planning coordinator	HHS Connection IT Governance Fiscal Year Planning

Document	Description	User Role	Location
PMRS Administrator Guide	Guide for the PMRS admin.	PMRS admin	Portfolio-Management Shared Drive
Time Effort Reporting Processes and Procedures	SharePoint page with procedures for Dovico, PPM, and Salesforce time effort reporting systems.	All roles	Time and Cost Allocation Procedures SharePoint Library
Time Effort Reporting – Work Hours per Month Resources	Outlines the minimum number of work hours full-time state resources should report in time effort reporting systems.	Time effort reporting administrator	Time and Cost Allocation Resources Library
Governmental Accounting Standards Board Accounting and Financial Reporting for Intangible Assets	Reporting requirements for the capitalization of projects.	All roles	Governmental Accounting Standards Board
DIR Project Financial Life Cycle Guide	DIR standards for project cost records.	All roles	DIR Website

6.3 Records

Records are electronically maintained for these processes in each of the referenced time effort reporting systems.

7 Database and System Applications

The following databases and system applications are used for this process.

Database or Application	Description	Location
Fiscal Year Planning	Used to develop and store fiscal year plans.	Fiscal Year Planning Application
PPM	Used to enter time related to projects.	PPM Log In Page
Dovico	Used to enter time related to projects.	Dovico Log In Page
Salesforce	Used to enter time related to projects.	Salesforce Log In Page

Database or Application	Description	Location
BASS	Used to enter time related to projects.	Local access database at OIG.
PMRS	Used to store project related documents and report the monthly status of projects with planned costs greater than or equal to $100,000.	PMRS Log In Page

Revision History

Date	*Change*	*Department Owner*
1/24/2018	***Revised***	***Business Operations and Project Management Office***
4/24/2017	***Revised***	***Project Management Office***
3/6/2018	***Revised***	***Project Management Office***
5/10/2016	***Revised***	***Project Management Office***
1/13/2015	***Issued***	***Project Management Office***

Request Revisions

Contact ***IT Planning, Policy, and Performance*** to request revisions to this document.

Appendix A: Acronyms

Acronym	Term
CAPPS	Centralized Accounting and Payroll/Personnel System
DIR	Department of Information Resources
HHS	Health and Human Services
HISS	HHS IT Statistics System
IT	Information Technology
ITBO	Information Technology Business Operations
OIG	Office of Inspector General
PMRS	Project Management and Repository System
PPM	Project and Portfolio Management

Exhibit I-5: Current TIERS PPM Installation Information

General Description:
The current TIERS MicroFocus Project and Portfolio Management (PPM) system is currently used by several HHS organizations for demand, project, and time management. It includes a real-time interface between the HHS Help Desk Remedy system and the PPM system. This interface integrates Remedy Support Tickets and PPM demand management maintenance requests. The Demand Management module is the primary work intake system for the largest HHS IT application support and maintenance department. New development work is managed with Request for IT Services (RITS), SR - Modification, and Action Item requests. New maintenance work is managed with SR - Maintenance requests. Each of these request types consist of customized resource assignments rules, workflow steps, and request statuses. Project Management and Time Management modules are used by several application support departments to manage individual IT project status and progress, resource assignments and activities, resource time sheets and monthly cost allocation metrics. The information provided below is derived from the HHS TIERS answers to the Micro Focus SaaS PPM migration questionnaire.

Installation Topic:	Details:
Current PPM Version:	9.42
Current PPM Service Pack	SP2
Current Operating System and database versions	Windows 2012, Oracle 11.2.0.4
Infrastructure details	We sit within the DMZ (the HHSC network). Prod environment is a 4-server cluster (3 user nodes, 1 services node), Test environment is standalone, Dev environment 3 server cluster (2 user nodes, 1 services node). Databases are all on RAC super cluster (3 node redundancy), we have a reporting database open to user queries and 2 additional standby databases
List of environments	Dev, Test, Production
Number of Users	1647

Installation Topic:	Details:
Current modules used & number of licenses for each module	Demand Management – 1395 Project Management – 346 Time Management – 1361 Foundation – 1 User Administration – 8 Configuration - 7
Current PPM processes and functionalities:	Project and budget management including planning Resource management Resource tracking (time management) Code Deliver (phasing out) Defect tracking (Service Request Maintenance and Modification requests) Release Management Requests for IT Services Environment Requests (Normal and production) Automated project creation from Modification and Release requests
Geography of current user base	All users are based in Texas, primarily users are located in Austin but also surrounding cities.
Use of web services	The Create Request is used to import requests from our Help Desk system (Remedy on Demand) to PPM prod.
Integration details	Tickets come into the help desk. Then, if they are escalated to level 2 they are sent to PPM via web services, resulting in the creation of the request in PPM via PPM web services (SOAP requests). Status, notes and field updates to the tickets in PPM are sent back to RoD via the same mechanism using the BMC Atrium Orchestrator adapters.
Sizing information of current installation	Projects – 3085 Requests – 784948 (updated daily) Timesheets -- 192597 Reports - 181086

Exhibit I-6: Other Legacy System Information

Legacy System:	**Dovico**
Description of system, including purposes fulfilled:	Dovico is a cloud-based timesheet and time tracking application. Dovico provides both employee time tracking and also project time tracking as well as project costing. We use Dovico reports for tracking total project time spent during a reporting period and from start of the project. We use this information when filling out PMRS. Since Dovico allows extensive categorization we can also track application maintenance, employee leave time, etc.
Number of Users:	Approximately 215
Confidential Data	Contains PII
Description of size of system (ex. # of records, storage size, etc.)	Since the application is hosted in the cloud it's hard to say exactly how much space the application and its data takes up, but we have records for several hundred employees and several thousand projects with daily time entries stretching back to September of 2005 when we first put it into service.

Legacy System:	**SalesForce**		
Description of system, including purposes fulfilled:	Application was created for the legacy DADS IT resources to capture timekeeping needs per project assigned. Currently the application is being used by the same resources who are not report under the IT MSS and Regulatory Services.		
Number of Users:	45		
Confidential Data	Contains none		
Description of size of system (ex. # of records, storage size, etc.)	Table (Object Name)	Record Count	Storage
	Timekeeping Projects	48	96 KB
	System Designators	66	132 KB
	Resources	155	310 KB
	Weekly Entries	13,314	26.0 MB
	Time Entries	115,068	224.7 MB

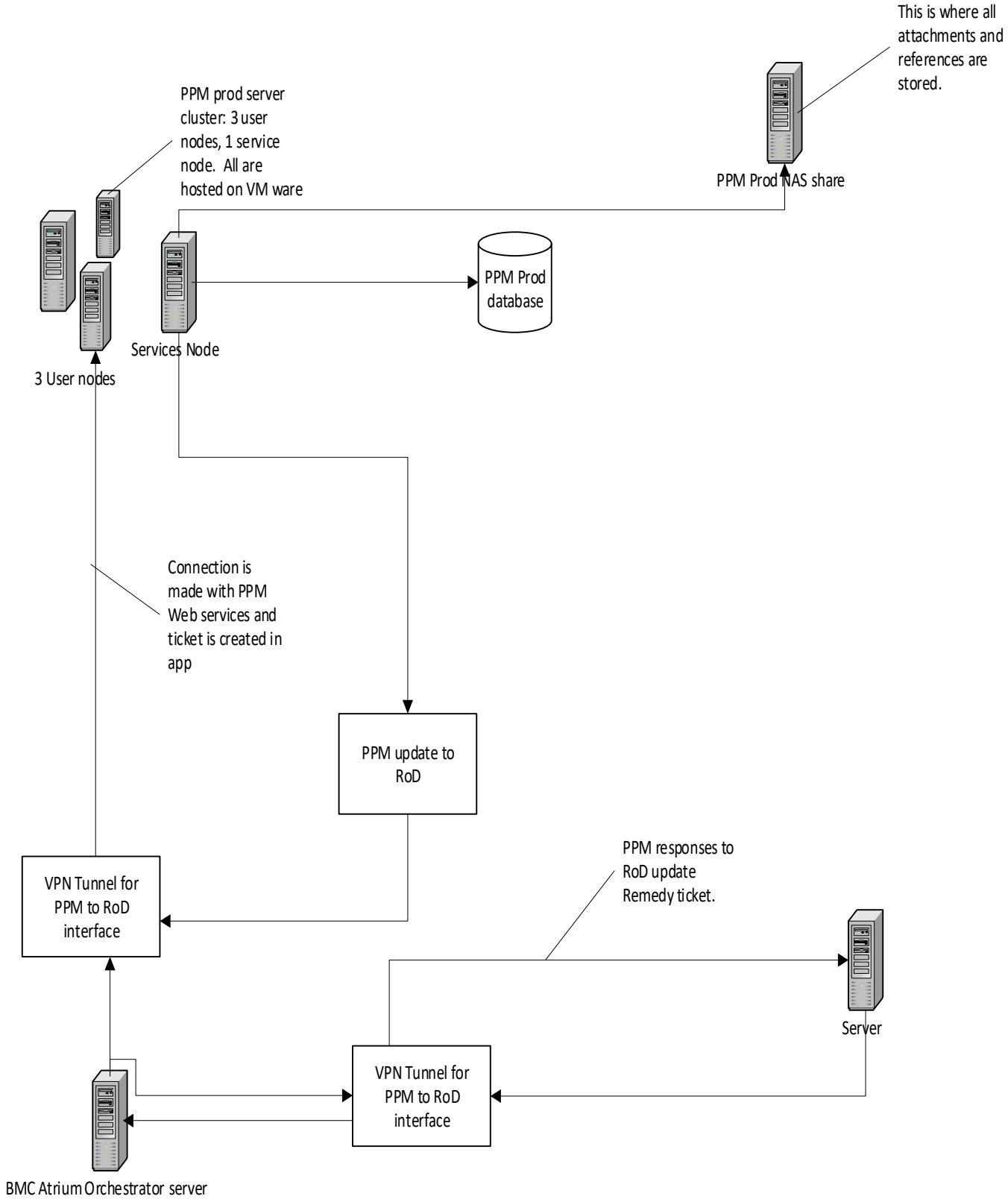
Legacy System:	**OIG Time Reporting**
Description of system, including purposes fulfilled:	The OIG TimeKeeper system allows OIG Data & Technology, OIG Chief Counsel, and HHSC IT Applications Support for OIG staff members to record the time they spend supporting the departments of OIG and report that time to HHSC Cost Allocation.
Number of Users:	~ 45-50

Legacy System:	**OIG Time Reporting**
Confidential Data	Contains PII
Description of size of system (ex. # of records, storage size, etc.)	There are currently 40,503 time keeping records in the database plus 1,000 reference table entries. The database takes up 26mb of disk storage.

Legacy System:	PMRS
Description of system, including purposes fulfilled:	The Project Management & Repository System (PMRS) is the web-based application used across the HHS Enterprise to report project status, archive project artifacts, monitor project progress, and manage work requests through the Project Management Life Cycle (PMLC.) PMRS provides: (Centralized access to processes, templates, and checklists, automated workflow from requests through project execution, online access to project artifacts and deliverables, standardized project status reporting, executive level status report summarization, status report data export functionality, search capability)
Number of Users:	120
Description of size of system (ex. # of records, storage size, etc.)	**Web Site**: 65,848 documents comprising 20GB **Oracle Database**: 58 Tables 50GB Prod/Last, 25GB Dev/Test

Legacy System:	FY Planning
Description of system, including purposes fulfilled:	Fiscal Year Planning is a RSA Archer application developed to track new IT initiatives and still in use due to flexible search and reporting tools. It is integrated with PMRS to fetch project status, cost, and start/end date changes every ten minutes. This is the system of record for approved IT initiatives/projects in each fiscal year since FY14.
Number of Users:	160
Description of size of system (ex. # of records, storage size, etc.)	There are approximately 300 fields per record and over 3200 records in this database, plus another 250k rows of change history to support those primary records.

Exhibit I-7: PPM Production Architecture


This is where all attachments and references are stored.
PPM prod server cluster: 3 user nodes, 1 service node. All are hosted on VM ware
PPM Prod NAS share
PPM Prod database
Services Node
3 User nodes
Connection is made with PPM Web services and ticket is created in app
PPM update to RoD
VPN Tunnel for PPM to RoD interface
PPM responses to RoD update Remedy ticket.
Server
VPN Tunnel for PPM to RoD interface
BMC Atrium Orchestrator server

.

Exhibit J: FFATA Certification

Texas Health and Human Services Commission
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 HHSC later determines that the Contractor knowingly rendered an erroneous certification, HHSC may pursue all available remedies in accordance with Texas and U.S. laws. 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.***

Did your organization have a gross income, from all sources, of less than $300,000 in your previous tax year?

☐ Yes - skip questions A, B, and C and continue to section D.

☐ No - answer questions A and B.

A. Certification Regarding Percent (%) 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 – skip question C.

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 – skip question C.

If your answer is Yes to both questions A and B, you must answer question C.
If you answer is No to either question A or B, skip question C and continue to section D.

C. Certification Regarding Public Access to Compensation Information.

Does the public have access to information about the highly compensated officers/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 - provide the names and total compensation of the top five highly compensated officers/senior executives using the attached FFATA Reporting Template.

D. Signatures

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.

Signature of Authorized Representative	
Printed Name of Authorized Representative	
Title of Authorized Representative	
Legal Name of Contractor	
Date	
DUNS Number	**Applicable HHSC Contract Number(s)** **[List all contract numbers in the cell above]**

Exhibit K: Certification Regarding Lobbying

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 L: Federal Assurances

OMB Number: 4040-0007
Expiration Date: 01/31/2019

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.

Previous Edition Usable

Authorized for Local Reproduction

Standard Form 424B (Rev. 7-97)
Prescribed by OMB Circular A-102

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

Standard Form 424B (Rev. 7-97) Back

Exhibit M: FNS Handbook 901 Federal Procurement Clauses

A11. Federal Procurement Clauses

A11.1 Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of federally assisted construction contract in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." (2 CFR 200, Subpart F, Appendix II)

The EEO clause must be included or the State must have its own EEO similar clause.

See the Department of Labor Executive Order 11246 – Equal Employment Opportunity for more information.

A11.2 Clean Air and Federal Water Pollution Control Act

Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended. Contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA). (2 CFR 200, Subpart F, Appendix II)

A11.3 Anti-Lobbying Act

This Act prohibits the recipients of Federal contracts, grants, and loans from using appropriated funds for lobbying the Executive or Legislative branches of the Federal government in connection with a specific contract, grant, or loan. As required by Section 1352, Title 31 of the U.S. Code and implemented at 2 CFR 200, Subpart F, Appendix II, for persons entering into a grant or cooperative agreement over $100,000, as defined at 31 U.S.C. 1352, the applicant certifies that:

a. 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 any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the making of any federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal grant or cooperative agreement;

b. 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 grantor o cooperative agreement, the undersigned shall complete and submit Standard Form – LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions;

c. The undersigned shall require that the language of this certification be include in the award documents for all sub-awards at all tiers (including sub-grants, contracts under grants and cooperative agreements, and subcontracts) and that all sub-recipients shall certify and disclose accordingly.

A11.4 Americans with Disabilities Act

See the Americans with Disabilities Act website for more information.

This Act (28 CFR Part 35, Title II, Subtitle A) prohibits discrimination on the basis of disability in all services, programs, and activities provided to the public and State and local governments, except public transportation services.

A11.5 Drug-Free Workplace Statement

The Federal government implemented 41 U.S. Code § 8103, Drug-free workplace requirements for Federal grant recipients in an attempt to address the problems of drug abuse on the job. It is a fact that employees who use drugs have less productivity, a lower quality of work, and a higher absenteeism, and are more likely to misappropriate funds or services. From this perspective, the drug abuser may endanger other employees, the public at large, or themselves. Damage to property, whether owned by this entity or not, could result from drug abuse on the job. All these actions might undermine public confidence in the services this entity provides.

Therefore, in order to remain a responsible source for government contracts, the following guidelines have been adopted:

1. The unlawful manufacture, distribution, dispensation, possession or use of a controlled substance is prohibited in the work place.
2. Violators may be terminated or requested to seek counseling from an approved rehabilitation service.
3. Employees must notify their employer of any conviction of a criminal drug statue no later than five days after such conviction.
4. Contractors of federal agencies are required to certify that they will provide drug-free workplaces for their employees.

Transactions subject to the suspension/debarment rules (covered transactions) include grants, subgrants, cooperative agreements, and prime contracts under such awards. Subcontracts are not included.

A11.6 Royalty Free Rights to Use Software or Documentation Developed

2 CFR 200.315 Intangible property.

(a) Title to intangible property (see §200.59 Intangible property) acquired under a Federal award vests upon acquisition in the non-Federal entity. The non-Federal entity must use that property for the originally-authorized purpose, and must not encumber the property without approval of the Federal awarding agency. When no longer needed for the originally authorized purpose, disposition of the intangible property must occur in accordance with the provisions in §200.313 Equipment paragraph (e).

(b) The non-Federal entity may copyright any work that is subject to copyright and was developed, or for which ownership was acquired, under a Federal award. The Federal awarding agency reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so.

(c) The non-Federal entity is subject to applicable regulations governing patents and inventions, including government wide regulations issued by the Department of Commerce at 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Awards, Contracts and Cooperative Agreements."

(d) The Federal Government has the right to:

(1) Obtain, reproduce, publish, or otherwise use the data produced under a Federal award; and

(2) Authorize others to receive, reproduce, publish, or otherwise use such data for Federal purposes.

A11.7 Debarment and Suspension

Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549. (2 CFR 200, Subpart F, Appendix II)

States to include in RFP and Contract a statement of certification by the vendor, such as "By signing this contract, the vendor certifies it is not suspended or debarred as specified by these rules."

Exhibit N: Insurance Requirements HHS0004417 Project and Portfolio Management Configuration & Implementation Services

Insurance Requirements HHS0004417 Project and Portfolio Management Configuration & Implementation Services

Vendor is required to submit Insurance and provide HHSC with proof of insurance, bonds, or both OR a reasonable alternative method with detailed explanation regarding inability of Vendor to obtain insurance/and or bonds, as per the information given below.

For the duration of any Contract resulting from this Solicitation, Vendor shall acquire insurance, bonds or both, with financially sound and reputable independent insurers, in the type and amount listed in the general insurance requirements. Failure to maintain insurance coverage or acceptable alternative methods of insurance shall be deemed a breach of Contract.

A. General Insurance Requirements

1. Contractor shall carry insurance in the types and amounts indicated in this for the duration of the Contract. The insurance shall be evidenced by delivery to System Agency 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, System Agency, and/or its agents, shall be entitled to receive without expense, copies of the policies and all endorsements.

2. 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 System Agency.

3. Contractor shall provide and maintain all insurance coverage with the minimum amounts described throughout the life of the Contract.

4. Failure to maintain insurance coverage, as required, is grounds for suspension of work for cause.

5. Contractor shall deliver to System Agency true and complete copies of certificates and corresponding policy endorsements upon award.

6. Failure of System Agency to demand such certificates or other evidence of Contractor's full compliance with these insurance requirements or failure of System Agency 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.

7. The insurance and insurance limits required herein shall not be deemed as a limitation on Contractor’s liability under the indemnities granted to System Agency in the Contract.

8. The insurance coverage and limits established below shall not be interpreted as any representation or warranty that the insurance coverage and limits necessarily will be adequate to protect Contractor.

9. 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 System Agency.

B. Policy Requirements.

1. This insurance shall not be canceled, materially changed, or non-renewed except after thirty (30) days written notice has been given to System Agency.

2. It is agreed that Contractor's insurance shall be deemed primary with respect to any insurance or self-insurance carried by System Agency for liability arising out of operations under the Contract with System Agency. Health and Human Services Commission, 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 System Agency. The additional insured status must cover completed operations as well. This is not applicable to workers' compensation policies.

3. A waiver of subrogation in favor of Health and Human Services Commission shall be provided in all policies.

4. Without limiting any of the other obligations or liabilities of Contractor, Contractor 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.

5. As an alternative, Contractor may include its Subcontractors as additional insureds on its own coverage as prescribed under these requirements. Contractor's certificate of insurance shall note in such event that Subcontractors are included as additional insureds and that Contractor agrees to provide workers' compensation for Subcontractors and their employees. Contractor shall obtain and monitor the certificates of insurance from each Subcontractor in order to assure compliance with the insurance requirements. Contractor 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.

C. Specific Insurance Coverage Required.

1. **Workers' Compensation**. Insurance with limits as required by the Texas Workers' Compensation Act, with the policy endorsed to provide a waiver of subrogation in favor of the Health and Human Services Commission, employer's liability insurance of not less than:

    a. $1,000,000 each accident;

b. $1,000,000 disease each employee; and
c. $1,000,000 disease policy limit.

Workers' compensation insurance coverage must be provided for all workers at all tier levels and meet the statutory requirements of Texas Labor Code.

2. **Commercial General Liability Insurance**. Including premises, operations, independent contractor'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 Contractor's liability for bodily injury (including death) and property damage with a minimum limit of:

   a. $1,000,000 per occurrence;
   b. $2,000,000 general aggregate;
   c. $5,000 Medical Expense each person;
   d. $1,000,000 Personal Injury and Advertising Liability;
   e. $2,000,000 products and completed operations aggregate;
   f. $50,000 Damage to Premises Rented to You; and
   g. Coverage shall be on an "occurrence" basis.

   The policy shall include endorsement CG2503 Amendment of Aggregate Limits of Insurance (per Project) or its equivalent.

   The term "You" as reference in Subsection above, means the Contractor.

3. **Comprehensive Automobile Liability Insurance**, 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**. Contractor shall obtain, pay for and maintain umbrella liability insurance during the Contract term, insuring Contractor for an amount of not less than amount $1,000,000 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. **Professional Liability Insurance**. Contractor shall obtain, pay for and maintain professional liability errors and omissions insurance during the Contract term, insuring Contractor for an amount of not less than $1,000,000.

6. **Cyber/Privacy Liability Insurance Policy**. Contractor shall provide Cyber/Privacy Liability Insurance to cover risk of loss to electronic data. The policy must include coverage 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.

Cyber Liability Insurance $1,000,000 Claim/$1,000,000 Aggregate.