



Dr. Courtney N. Phillips, Executive Commissioner

**STATEMENT OF WORK
Assessment of Health & Human Services Information Technology
Organizational Maturity**

Under DBITS IT Assessments/Planning Category

SOW No. HHS0007041

**Date of Release: 12/12/2019
Responses Due: 01/02/2020 by 2 p.m. CST**

Contents

1. Introduction	8
2. SOW Solicitation Overview.....	8
2.1. Project Description.....	8
2.2. SOW Solicitation Point of Contact.....	9
2.3. SOW Solicitation Schedule	9
2.4. Questions and Answers	10
2.5. SOW Solicitation Contents.....	10
3. Services Description.....	11
3.1. Scope of Services	11
3.1.1. Objectives of the Services	11
3.1.2. Specific Background Related to this SOW	11
3.2. Project Period	12
3.3. Project Milestones and Deliverables	13
3.4. Additional Project Deliverables	17
3.4.1 Key Personnel – Project Manager	17
3.4.2 Weekly Status Report	17
3.4.3 Issue Log	17
3.4.4 Risk Log.....	18
4. Deliverables.....	18
4.1 Deliverables Format.....	18
4.2 Deliverables Acceptance Criteria	19
4.3 Deliverable Due Dates	19
4.4 Deliverable Review Process	19
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 Presentations	21
6.4 Performance Measures and Associated Remedies	21
6.5 Service Level Agreements (SLAs)	21
7. Invoices.....	22
8. HHSC/Vendor-Furnished Equipment and Work Space.....	22
8.1 Restrictions on Access and Use	22
8.2 Vendor Furnished Equipment and Work Space	23
9. Contractor Warranties.....	23
9.1 General	23
10. Project Termination.....	23
10.1 For Convenience.....	23
10.2 Immediate Termination	23

10.3	Notice to Cure	24
10.4	Effect of Termination	24
11.	Liability	24
11.1	Acknowledged Direct Damages	24
11.2	Limitation of Liability	25
12.	SOW Solicitation Additional Terms and Conditions	25
12.1	Exceptions to Terms	25
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	26
12.6	Property of HHSC	26
12.7	Copyright Restriction	26
12.8	Texas Public Information Act Applicable to Responses	26
12.9	TEC Form 1295	27
13.	Response Submission Instructions	27
13.1	Number of Copies	27
13.2	Time and Place of Submission	27
14.	Response Organization and Content	27
14.1	Overview	27
14.2	Part 1 – Required Acknowledgments	28
14.3	Part 2 – Qualifications and Background	28
14.4	Part 3 – Technical Proposal	29
14.5	Part 4 – Price Proposal	30
14.6	Exceptions to Terms and Conditions	31
15.	Historically Underutilized Business Participation	31
16.	Response Evaluation	31
16.1	Conformance with State Law	31
16.3	Specific Criteria	31
16.4	Questions or Requests for Clarification by HHSC	32
16.5	Oral Presentations	32
16.6	Best and Final Offers	32
16.7	Discussions with Responding Vendors	32
16.8	Award	32
17.	Additional Terms and Conditions	32
17.1	External Factors	32
17.2	Standards of Conduct	33
17.3	U.S Department of Homeland Security’s E-Verify System	33
Exhibit A. HEALTH AND HUMAN SERVICES CONTRACT AFFIRMATIONS		35
Exhibit B: HHS Information Security Acceptable Use Policy (HHS AUP):		47
Exhibit C: Health and Human Services Acceptable Use Agreement (AUA):		57
Exhibit D: HHS System Data Use Agreement		66
Exhibit D-1: HHS System Security and Privacy Inquiry (SPI)		79
Exhibit E: Experience Reference Form		98
Exhibit E-1: RESPONDENT RELEASE OF LIABILITY		101
Exhibit F: Vendor Price Sheet		102

Exhibit G: HHSC Uniform Terms and Conditions	104
Exhibit G-1: HHSC Special Conditions	129
Exhibit H: Scope of Work Supporting Documents	140
Exhibit H-1: HHSC IT Organizational Structure.....	141
Exhibit H-2: Glossary.....	150
Exhibit H-3: DRAFT Support Services Agreement.....	152
SECTION 1 – Preamble	152
SECTION 2 – Overview	152
A. Overview of HHSC Information Technology	152
B. Organization Chart for the Information Technology (FY19)	154
SECTION 3 – Requestable Services	154
A. Applications	155
A.1. SharePoint	155
A.2. TxEVER (Texas Electronic Vital Events Registrar) Help Desk	155
A.3. TIERS Help Desk.....	155
A.4. Salesforce—Application Development.....	155
A.5. Application Modification	156
A.6. New IT Application	156
A.7. Medicaid Management Information System (MMIS) Enhanced Funding	156
A.8. Request for Proposal (RFP) Creation for IT Applications	156
A.9. Contract Consulting for IT Applications.....	157
B. Business Operations	157
B.1. Procurement Approach Consulting	157
B.2. Procurement Project Management	157
B.3. Procurement Business Analysis	157
B.4. Statement of Work/Request for Offers/Request for Proposals Drafting	158
B.5. Federal and State Reporting and Coordination.....	158
C. Chief Technology Office	158
C.1. Business Architecture Engagement.....	158
C.2. Architecture Consultation.....	159
C.3. Applications Architecture Strategy	159
C.4. Enterprise System Architecture	159
D. IT Chief Information Security Office (CISO)	159
D.1. System Categorization, Project Support, and Procurement Support	159
D.2. System Security Plans and Information System Risk Assessments	160
D.3. Vulnerability Assessments and Penetration Testing	160
D.4. Independent Security Assessments	160
D.5. Contract Oversight and Monitoring Advice	160
D.6. Audit Support.....	160
D.7. Information Security Awareness Program	161
D.8. Incident Response	161
E. Converged Services	161
E.1. Virtual Private Network (VPN).....	161
E.2. Contact Center Services	161
E.3. Basic and Advanced Phone Service	162

E.4. Teleconferencing—Public Hearing Teleconferencing (PHTC)	162
F. Customer Service and Support	162
F.1. Health and Specialty Care Systems Customer Support	162
F.2. IT Customer Service Help Desk	162
F.3. Regional and State Office Customer Support	163
G. Data Center Services	163
G.1. DCS Delivery	163
G.2. DCS Disaster Recovery Services	163
G.3. DCS-Enterprise Secure FTP Support (SFTP)	164
G.4. DSHS and HHSC DCS-Resource Management	164
G.5. DCS-Enterprise Reporting Mental and Behavioral Health Outpatient Warehouse (MBOW) Data Warehouse Support	165
H. IT Governance	165
H.1. IT Governance Office	165
I. System Services	165
I.1. Network Provisioning Services	165
I.2. Password Manager Enterprise Single Sign-on (ESSO)	166
I.3. Access Management	166
I.4. Application Provisioning Services	166
I.5. Video Conference Service	166
I.6. Hardware Asset Management	166
I.7. Automation and Image Management	167
I.8. Software Asset Management (SAM)	167
I.9. Local Office Infrastructure (LOI)	167
I.10. New Cellular Services Accounts	167
I.11. Cellular Services	167
I.12. Teleconferencing—Audio/Video Teleconferencing	168
I.13. Related Services - Language Support	168
I.14. Incident Management Processes/Communication/Restoration/Remedial Action	168
I.15. E-Discovery Services	168
SECTION 4 – HHS Support Services	169
1. Continuous Monitoring	169
2. Information and Data Architecture	169
3. New and Emerging Technology, Proof of Concepts, Application Pilots and Reference Implementations	170
4. Local Area Network (LAN)	170
5. Wide Area Network (WAN)	170
6. Wireless Local Area Network (WLAN)	171
7. Perimeter (Access and Security)	171
8. Customer Care	171
9. DCS TIERS Operations	172
10. IT DCS-Winters Data Center	172
11. IT Staff Augmentation Support	172
12. IT Contract Support	172

13. Directory Services	173
14. Email/Security	173
15. Office 365 (O365) Services/Collaboration Tools/Authentication.....	173
SECTION 5 – Roles and Responsibilities	173
SECTION 6 – Approval of Contracts for Support Services	176
SECTION 7 – Performance Goals and Measures	176
SECTION 8 – Administrative Support Service by Alternative Means	176
SECTION 9 – Staffing Implications	177
SECTION 10 – Performance Reporting.....	177
SECTION 11 – Escalation	177
SECTION 12– Attachments.....	177
SECTION 13 – Expiration and Modification.....	177
SECTION 14 – Points of Contact.....	177
SECTION 15– Signature.....	178
ADDENDUM 1	179
A. IT Compliance Services	179
A.1. Medicare Information Technology Architecture (MITA) Assessments	179
A.2. Medicaid Managed Information System (MMIS) Certification	179
B. IT Planning Services	179
B.1. MITA Architecture	179
B.2. Medicare Information Technology Architecture (MITA) Assessments	180
B.3. Medicaid Managed Information System (MMIS) Certification	180
B.4. Interoperability Roadmap Development.....	180
B.5. Interoperability and Standards	180
ATTACHMENT A - HHSC IT Application Service Levels.....	181
ATTACHMENT B - Priority Levels	184
ATTACHMENT C - Applications	185
Supported by HHSC IT by Governance Portfolio	185
Administrative Portfolio	185
Health and Specialty Care System Portfolio	187
Inspector General Portfolio	188
Medical and Social Services Portfolio - Access & Eligibility Services Sub Portfolio	188
Medical and Social Services Portfolio - Health, Developmental & Independence Services Sub Portfolio.....	189
Medical and Social Services Portfolio - Intellectual and Developmental Disabilities & Behavioral Health Services Sub Portfolio	190
Medical and Social Services Portfolio - Medicaid & CHIP Services Sub Portfolio	190
Medical and Social Services - Other	191
Public Health Services Portfolio	191
Regulatory Services Portfolio	192
ATTACHMENT D - Service Level of System-Wide Applications	193
ATTACHMENT E - Service Level for MSS Division-Specific Applications	194
Exhibit I: FFATA Certification	199
Exhibit J: Certification Regarding Lobbying.....	202
Exhibit K: Federal Assurances	203

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**” or “**HHS**”). 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 assess the current organizational maturity of the HHS (both DSHS and HHSC) IT department, and to provide recommendations on steps that the IT department should implement to achieve a future state higher organizational maturity level. This SOW describes specific topics that HHSC expects the selected Vendor to address for assessment and evaluation of the organizational maturity of the IT department, however vendors should feel free to propose additional areas of focus, maturity assessment methodologies, and/or maturity assessment models as part of the vendor’s technical proposal, as discussed further below.

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. In all other respects, the terms and conditions of this SOW supersede and control. Refer to **Appendix A** of Vendor’s DIR Contract, **Exhibit H** of this SOW, **Exhibit G, HHSC Uniform Terms and Conditions**, and **Exhibit H-1** of this SOW, **Exhibit G-1, HHSC Special Conditions**, for defined terms in addition to those defined herein.

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**”).

2. SOW Solicitation Overview

2.1. Project Description

HHSC is undertaking a project to assess the current HHS IT department organizational maturity and to develop actionable and feasible recommendations on increasing the maturity level of the HHS IT organization. HHSC seeks a qualified vendor to complete the project as a deliverables-based engagement. The project activities are comprised of three (3) milestones. The selected Vendor must complete the three (3) milestones within six (6) months from the effective date of the Contract. The vendor may perform optional screening of their proposed personnel as required to meet due diligence in hiring personnel. The vendor is to provide information on the screening and/or background check process that is performed before a staff is hired. This requirement does not mean that the vendor is to provide the results of the screening and/or background check on any specific proposed personnel that they have performed.

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. Vendor will primarily work off-site due to space limitations at state facilities, with the selected vendor providing secure online file sharing or "drop box" capabilities, outside of the HHS network, utilized by HHS and Vendor as needed to provide and exchange documentation during the engagement. This SOW does not include reimbursable travel expenses.

HHSC has included **Exhibit H-1** to this SOW that describes the organizational structure of HHSC IT 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 Solicitation 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
December 12, 2019	Distribute SOW to prospective vendors
January 2, 2020 [2 pm]	Vendor deadline for submitting questions to HHSC
January 9, 2020	Anticipated HHSC response to questions
January 23, 2020 [2 pm]	Vendor deadline for submitting responses to SOW
February 13, 2020	Anticipated award
March 12, 2020	DIR review completed
March 20, 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: HHS Information Security Acceptable Use Policy (HHS AUP);
Exhibit C: Health and Human Services Acceptable Use Agreement (AUA);
Exhibit D: HHS System Data Use Agreement ver. 8.5;
Exhibit D-1: HHS Security and Privacy Inquiry (SPI);
Exhibit E: Experience Reference Form;
Exhibit E-1: Respondent Release of Liability;
Exhibit F: Vendor Price Sheet;
Exhibit G: HHSC Uniform Terms and Conditions;
Exhibit G-1: HHSC Special Conditions;
Exhibit H: Scope of Work Supporting Documents;
Exhibit H-1: HHSC IT Organizational Structure;
Exhibit H-2: Glossary;
Exhibit H-3: DRAFT Support Services Agreement
Exhibit I: FFATA Certification;
Exhibit J: Certification Regarding Lobbying; and
Exhibit K: Federal Assurances

3. Services Description

3.1. Scope of Services

3.1.1. Objectives of the Services

HHSC seeks a qualified Vendor to perform a comprehensive assessment of the organizational maturity level of the HHS IT department, following which the Vendor will provide a comprehensive set of recommended actions and roadmap for increasing the maturity level of the HHS IT organization. The Vendor will specifically include the following areas of analysis in its assessment; prospective vendors may propose additional areas of analysis that are industry-recognized areas of concern for IT organizational maturity.

1. Service Delivery – Level and quality of current service delivery to internal agency program areas.
 - a. Reviews how and to what quality services are currently delivered
 - b. Looks at the process integration, management of the service and the use of service level agreements
2. Price Point – Cost to the IT organization to deliver services. Compares the internal cost of providing services against that of other state and federal agency IT organizations
3. People – Quality of staff delivery
 - a. Reviews the definition of roles and responsibilities, employee care and ongoing improvement of skills
4. Measurement – Management and analysis of performance metrics
 - a. Reviews how the organization tracks metrics and the use of key performance indicators
 - b. Reviews how an organization uses these lessons within a root-cause analysis program or continuous improvement
5. Financial Management – Financial controls and discipline
 - a. Reviews the way the organization deals with budgetary and cost considerations across the disciplines, includes the consideration of automated approvals, cost allocations, etc.
6. Standardization – Level of standardization across technical landscape
 - a. Reviews the consistency in the application and use of systems, processes and tools to promote efficiency and effectiveness.
7. Tools and Automation – Quality and automation of current toolset
 - a. Reviews the tools in place, both in terms of completeness of solution, as well as usability and automation.

3.1.2. Specific Background Related to this SOW

The Health and Human Services Information Technology organization is currently headed by the Deputy Executive Commissioner for IT, who is also acting as Interim Chief Information Officer (CIO). The organizational structure is provided in chart form in **Exhibit H-1, HHS IT Organizational Structure**. The HHS IT Division is comprised of the Deputy CIO for Governance and Enterprise Relationship Management, the Deputy CIO for IT Strategy and Chief Technology Officer, the Department of State Health (DSHS) Resources Manager and

Information Resource Manager, the Chief Information Security Office, IT Business Operations, IT Infrastructure, IT Project Management Office and Application Services.

The Chief Information Security Office is comprised of the Chief Information Security Officer (CISO); the DSHS CISO; the Information Security Officer, Risk; Cybersecurity Operations Officer and IT Security Analysts.

The IT Business Operations (ITBO) is comprised of the following areas: Procurement Projects and Support; Procurement and Contracting Support; Federal/State Reporting Coordination; Workforce Support; Budget Management and Forecasting; Planning, Policy and Performance plus an additional 6 staff that report directly to the ITBO director.

The IT Infrastructure is comprised of the following areas: IT Data Center Services and Operations; Customer Service and Support; Converged Services; System Services; Operations Management.

The IT Project Management Office (PMO) is comprised of a Deputy PMO Director, a Project and Program Support Office and an additional director.

The Application Services area is managed by a director and deputy director and is comprised of staff and contractors in the following portfolios: Administrative Applications; Medical and Social Services Applications; Social Services Applications; Public Health Applications (DSHS); Data Analytics Support; Inspector General Applications; Health and Specialty Care System Applications; Regulatory Applications.

HHS has just introduced its inaugural business plan, the [Blueprint for a Healthy Texas](#). Contained within this business plan is Initiative 12: Technology & Innovation Leverage Technology and Process Improvement, which defines the immediate future initiatives for the IT Division.

HHS IT, in compliance with Texas Government Code Sections 531.02012 and 531.00553, has developed a support services agreement (SSA) that outlines, at a high level, the centralized services that the Health and Human Services Commission (HHSC) will receive from HHSC Information Technology. This SSA also includes performance goals that the HHS Information Technology department must meet and defines the fundamental roles and responsibilities of the respective areas related to Information Technology services. A copy of an abbreviated and draft SSA is attached as **Exhibit H-3: DRAFT Support Services Agreement**.

The HHSC CIO position is currently held by an interim CIO. The CIO position has been held by an acting or interim CIO for 11 of the last 23 months.

3.2. Project Period

Vendor is required to complete the Services over a contiguous six (6) 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. If HHSC elects to extend the Contract, during the extension term the Parties will enter into an Amendment adding the applicable Change

Request Plan, including added Deliverables and applicable Vendor costs to HHSC, as defined by **Section 5** of this SOW. 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 specifically set forth in the Contract.

3.3. Project Milestones and Deliverables

Vendor will perform the Services using a project milestone approach, as generally described below. In completing each of the milestones, Vendor will assess and evaluate the current IT Organizational Maturity to provide recommendations on maturing the HHS IT Organization. provided in **Exhibit H**. The Project Schedule (defined below in **Section 4.3**) indicates when each of the project milestones and Deliverables are to be completed.

Milestone 1 - Assessment

Contractor's Milestone 1 tasks include:

- Provide a 5-level IT organizational maturity model containing specific evaluation criteria and defined metrics that Vendor will use as the basis from which to assess and determine the current maturity level of HHS's IT organization based upon past and current studies related to organizational maturity; this IT organizational maturity model will also serve as the reference for Vendor's recommendations for achieving increased IT organizational maturity to be provided by Vendor as part of Milestone 3.
- Develop a comprehensive assessment methodology to evaluate HHS's current IT organizational maturity level using the following framework listed in **Section 3.1.1. Objective of Services**.
- Determine the participants for the IT organizational maturity (see organization charts in **Exhibit H-1**) for the structure and counts of full-time equivalents positions
- Develop a communications plan for ongoing status, findings and recommendations
- Perform a survey of HHS's IT organizational maturity performance using questionnaires sent to all staff identified in previous task
- Validate the results of the questionnaires through interviews, focus groups and archive reviews
- Build support for implementing recommendations

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

Deliverable No.	Deliverable	Acceptance Criteria
D.1.1	A 5-level organizational model	A 5-level framework ranging from basic to sophisticated practices

Deliverable No.	Deliverable	Acceptance Criteria
D1.2	A comprehensive and documented assessment methodology	A collection of reliable, proven processes (e.g., surveys, document reviews, data analysis, interviews, staff meetings) tailored to achieve the Project objectives in relation to the HHS IT organization.
D1.3	A list of participants for the survey(s) and interviews	A list of the IT and other HHS staff employees identified by Vendor to participate in a Vendor-developed survey and then a second list of employees for the results validation meetings including an explanation on how the participants were chosen.
D1.4	Communication Plan & Escalation Strategy	Definition of detail communications between Vendor and HHSC, how issues will be tracked, mitigated and escalated. The escalation chain needs to be identified and defined for both the Vendor and HHSC.
D1.5	A completed survey summary to evaluate and document the current organizational maturity	Documented results of the survey evaluating the organizational maturity using recognized and approved methodology.
D1.6	Validation interview and focus group results summary	Documented results of the validation interviews and focus groups undertaken following the completion of the survey to verify the survey results.
D1.7	A summary of items reviewed in archive review process	Documented summary of archive items reviewed, the subject of those items and how they related to the organizational maturity assessment.
D1.8	Milestone Closeout	Assessment of the milestone to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the milestone has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted.

Milestone 2 - Evaluation

Contractor's Milestone 2 tasks include:

- Analyze the collected information gathered for Milestone 1 to evaluate and benchmark HHS's current IT processes and practices maturity level using specific criteria
- Identify HHS's IT organizational strengths and weaknesses in terms of IT processes and practices
- Search for any "success drivers" by testing for correlations between different areas of the HHS IT organization's maturity levels
- Determine HHS IT Department's current level of organizational maturity

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

Deliverable No.	Deliverable	Deliverable Description
D2.1	A list of HHS's IT organizational strengths and weaknesses in terms of IT processes and practices	IT organizational strengths and weaknesses identified during the organizational maturity assessment identified by both IT department and organizational maturity assessment category.
D2.2	Identified "success drivers"	"Success drivers" for organizational maturity identified during the organizational maturity assessment identified by both IT department and organizational maturity assessment category.
D2.3	A roadmap for organizational improvement	Recommendations for each IT department on specific activities to increase the organizational maturity based upon the specific findings for each department. Any "success drivers" that have been identified within the organization should be identified as improvement facilitators, when appropriate, to make suggested improvements in other departments or areas of IT.
D2.4	Organizational change management tools, plans to aid in the implementation of recommendations	Document steps/guidance on how to market/communicate/implement the recommended changes to increase the organizational maturity and marketing aids to facilitate in growing the organizational maturity.
D2.5	Documented current level of organizational maturity	A complete summary of all steps, activities and findings to determine the current level of organizational maturity on the 5-level framework on organizational maturity within each area of the maturity framework listed in Section 3.1.1. Objective of Services.

Deliverable No.	Deliverable	Deliverable Description
D2.6	Milestone closeout	Assessment of the milestone activities to ensure completion and derive any lessons learned and best practices to be applied to future projects; to confirm the milestone has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted.

Milestone 3 - Findings and Recommendations

Contractor will provide:

- Draft, prioritize and communicate the findings of the assessment
- Develop specific, tailored, actionable recommendations
- Communicate findings and recommendations to all levels of participants in the assessment through webinars, emails, documents and any other means deemed appropriate

Contractor will produce these deliverables:

Deliverable No.	Deliverable	Deliverable Description
D3.1	Findings	A document summarizing all strengths and weaknesses in the IT organization relating to organizational maturity.
D3.2	Recommendations	Specific recommendations addressing each of the identified weaknesses in how to move forward to increase the organizational maturity regarding these weaknesses and how to leverage the identified strengths to improve organizational maturity in each department and in the IT organization within each area of the maturity framework listed in Section 3.1.1. Objective of Services.

Deliverable No.	Deliverable	Deliverable Description
D3.3	Milestone Closeout	Assessment of the milestone to ensure completion, and derive any lessons learned and best practices to be applied to future projects; to confirm the milestone has met all sponsor, customer, and stakeholder requirements, verifying that all deliverables have been delivered and accepted.

3.4. Additional Project Deliverables

3.4.1 Key Personnel – Project Manager

In addition to any other key personnel identified by Vendor in Vendor's Response, Vendor shall provide a qualified Project Manager to serve as single point of contact and coordinate all project tasks with the HHSC Project Manager. The Vendor Project Manager will provide quality assurance and oversight for all Services. The Vendor Project Manager will identify and schedule Vendor resources to meet project Deliverables and the Project Schedule. The Vendor Project Manager identified in Vendor's Response to this SOW Solicitation shall serve as the Vendor Project Manager and Vendor shall not reassign or remove the designated individual or any other key personnel without HHSC's prior written consent, except for reasons for cause or discipline. In the event that any key personnel role becomes vacant, Vendor shall fill the role with a suitably qualified individual within five (5) business days. Vendor shall provide HHSC information on the skills, experience, and qualifications of any proposed replacement key personnel, and HHSC shall have the right to reject any proposed replacement Project Manager that HHSC determines, in its sole discretion, does not meet the required qualifications of this SOW.

3.4.2 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 milestone 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.

3.4.3 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.

3.4.4 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 HHS 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 H**, as verified and corrected/completed by deliverables D1.8, D2.6 and D3.3.
- 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-through 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 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.

6.4 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.

6.5 Service Level Agreements (SLAs)

HHSC contracts for results. A successful result may be defined as the generation of discrete, defined, measurable, and beneficial outcomes that support HHSC Statement of Work goals, service delivery agreements, and product specifications. HHSC will monitor the performance of a contract issued under this SOW. All services and work products under the Contract shall conform to this SOW at an acceptable quality level and in a manner consistent with acceptable industry standard, custom, and practice. HHSC will monitor Vendor's conformance to Deliverables due dates and adherence to the Project Schedule. HHSC will have the right and option to assess liquidated damages for Vendor's failure to meet SLAs as specified in the table below.

SLA	SLA Name	Performance Evaluated	Non-Conformance	Frequency of Measurement
SLA 1	Deliverable Timeliness	100% of all Deliverables identified in Section 3.3 must be submitted by the date specified in the HHSC-accepted Work Plan	Liquidated Damages in the amount of \$250 for each day of non-conformance, not to exceed \$5,000 in any given month.	Monthly

7. Invoices

Vendor may submit invoices on a monthly basis for completed Deliverables accepted by HHSC during the preceding calendar month as provided herein. 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 milestones 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 B, HHS Information Security Acceptable Use Policy (AUP)**, **Exhibit C, Health and Human Services Acceptable Use Agreement (AUA)**, and **Exhibit D, HHS System Data Use Agreement**, and subject to successful completion by Vendor of **Exhibit D-1, HHS System Security and Privacy Inquiry**, HHSC will make the 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 HHSC's sole discretion upon notice to Vendor by HHSC.

8.2 Vendor Furnished Equipment and Work Space

Vendor is to remotely perform Services using Vendor equipment in a Vendor-controlled environment. 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 B, C, and D** 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.

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 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 for cause 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 D, HHS System 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 D, HHS System 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, Texas Government Code, Chapter 552, including those provisions applicable to third-party information (including third-party, proprietary information) received by a state agency. 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. 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.

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 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/filinginfo/1295/>

13. Response Submission Instructions

13.1 Number of Copies

Respondent must submit one electronic copy of the Response, 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 Responses submitted by telephone and facsimile.

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 the Response to HHSC's Procurement and Contracting Services (PCS) Division no later than **January 23, 2020** at 2:00 P.M., CST. All Responses 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 Response submissions. It is the Respondent's responsibility to appropriately mark and deliver the Response 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 **Exhibit A, Contract Affirmations and Solicitation Acceptance**;
- b. Acknowledgment of schedule acceptance as described in **Section 3.2**;
- c. Acknowledgement of acceptance of all terms and conditions of the SOW; and
- d. 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 IT Organizational Maturity Assessment experience.

b. 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.

c. 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 E, 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 E-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

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. This section should include Vendor's proposed reference model for measuring IT department organizational maturity, and any related proposed modifications or additions to the project deliverables to best achieve the project objectives. 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 milestone;
- 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 Weekly Status Report

d. Sample Issue Log

e. Sample Risk Log

f. Sample Communication Plan

g. 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 F, Vendor Price Sheet**, and include Vendor's Price Sheet with Vendor's Response as a separate file or document.

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.

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. Response 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.

16.3 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

HHSC may require an oral presentation from any or all responding Vendors. Responding Vendors will be provided with advance notice of any such oral presentation and are responsible for their own presentation equipment. Failure to participate in the requested presentation may eliminate a 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.

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.

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 milestones 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 HHS 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.**

Exhibit A. HEALTH AND HUMAN SERVICES CONTRACT AFFIRMATIONS

HEALTH AND HUMAN SERVICES CONTRACT AFFIRMATIONS

The term "System Agency" used in these affirmations means HHS or any of the agencies of the State of Texas that are overseen by HHSC under authority granted under Texas law and the officers, employees, authorized representatives, and designees of those agencies. These agencies include: HHSC and the Department of State Health Services.

By entering into this Contract, Contractor affirms, without exception, understands, and agrees to comply with the following items through the life of the Contract:

1. Contractor represents and warrants that these Contract Affirmations apply to Contractor and all of Contractor'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 Contract and any related Solicitation.
2. **Complete and Accurate Information**
Contractor represents and warrants that all statements and information provided to System Agency are current, complete, and accurate. This includes all statements and information in this Contract and any related Solicitation Response.
3. **Public Information Act**
Contractor understands that System Agency 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 Contract or any related Solicitation may be subject to public disclosure pursuant to the Texas Public Information Act. In accordance with Section 2252.907 of the Texas Government Code, Contractor 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. **Contracting Information Requirements**
Contractor 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 Contractor agrees that the Contract can be terminated if the Contractor knowingly or intentionally fails to comply with a requirement of that subchapter.

5. Assignment

- A. Contractor 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.
- B. 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. Upon receipt of System Agency's notice of assignment, pledge, or transfer, Contractor shall cooperate with System Agency in giving effect to such assignment, pledge, or transfer, at no cost to System Agency or to the recipient entity

6. Terms and Conditions Attached to Response

Contractor accepts the Solicitation terms and conditions unless specifically noted by exceptions advanced in the form and manner directed in the Solicitation, if any, under which this Contract was awarded. Contractor agrees that all exceptions to the Solicitation, as well as terms and conditions advanced by Contractor that differ in any manner from System Agency's terms and conditions, if any, are rejected unless expressly accepted by System Agency in writing.

7. System Agency Right to Use

Contractor agrees that System Agency has the right to use, produce, and distribute copies of and to disclose to System Agency employees, agents, and contractors and other governmental entities all or part of this Contract or any related Solicitation Response as System Agency deems necessary to complete the procurement process or comply with state or federal laws.

8. Release from Liability

Contractor generally releases from liability and waives all claims against any party providing information about the Contractor at the request of System Agency.

9. Dealings with Public Servants

Contractor 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 Contract or any related Solicitation, or related Solicitation Response.

10. Financial Participation Prohibited

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

11. Prior Disaster Relief Contract Violation

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 Contractor certifies that the individual or business entity named in this Contract and any related Solicitation Response is not ineligible to receive this Contract and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.

12. Child Support Obligation

Under Section 231.006(d) of the Texas Family Code regarding child support, Contractor certifies that the individual or business entity named in this Contract and any related Solicitation 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.

13. Suspension and Debarment

Contractor 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 Contractor's subcontracts, if any, if payment in whole or in part is from federal funds.

14. Excluded Parties

Contractor 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.'

15. Foreign Terrorists Organizations

Contractor 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.

16. Executive Head of a State Agency

In accordance with Section 669.003 of the Texas Government Code, relating to contracting with the executive head of a state agency, Contractor 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 this 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.

17. Human Trafficking Prohibition

Under Section 2155.0061 of the Texas Government Code, Contractor certifies that the individual or business entity named in this Contract is not ineligible to receive this contract and acknowledges that this Contract may be terminated and payment withheld if this certification is inaccurate.

18. Franchise Tax Status

Contractor 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.

19. Debts and Delinquencies

Contractor agrees that any payments due under this Contract shall be applied towards any debt or delinquency that is owed to the State of Texas.

20. Lobbying Prohibition

Contractor represents and warrants that payments to Contractor and Contractor's receipt of appropriated or other funds under this Contract or any related 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).

21. Buy Texas

Contractor 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.

22. Disaster Recovery Plan

Contractor agrees that upon request of System Agency, Contractor shall provide copies of its most recent business continuity and disaster recovery plans.

23. Technology Access

- A. Contractor 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, Contractor represents and warrants to System Agency that the technology provided to System Agency for purchase (if applicable under this Contract or any related Solicitation) is capable, either by virtue of features included within the technology or because it is readily adaptable by use with other technology, of:
 - i. providing equivalent access for effective use by both visual and non-visual means;
 - ii. presenting information, including prompts used for interactive communications, in formats intended for non-visual use; and
 - iii. being integrated into networks for obtaining, retrieving, and disseminating information used by individuals who are not blind or visually impaired.
- B. 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.

- C. 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.

24. Computer Equipment Recycling Program

If this Contract is for the purchase or lease of computer equipment, then Contractor 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.

25. Television Equipment Recycling

If this Contract is for the purchase or lease of covered television equipment, then Contractor certifies that it is compliance with Subchapter Z, Chapter 361 of the Texas Health and Safety Code related to the Television Equipment Recycling Program.

26. Cybersecurity Training

- A. Contractor 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.
- B. Contractor represents and warrants that if Contractor or Subcontractors, officers, or employees of Contractor have access to any state computer system or database, the Contractor, Subcontractors, officers, and employees of Contractor shall complete cybersecurity training pursuant to and in accordance with Government Code, Section 2054.5192.

27. Restricted Employment for Certain State Personnel

Contractor 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 Contractor may not accept employment from Contractor before the second anniversary of the date the Contract is signed or the procurement is terminated or withdrawn.

28. Disclosure of Prior State Employment

If this Contract is for consulting services under Chapter 2254 of the Texas Government Code, in accordance with Section 2254.033 of the Texas Government Code, Contractor certifies that it does not employ an individual who was employed by System Agency or another agency at any time during the two years preceding the submission of any related

Solicitation Response related to this Contract or, in the alternative, Contractor has disclosed in any related Solicitation Response the following:

- i. the nature of the previous employment with System Agency or the other agency;
- ii. the date the employment was terminated; and
- iii. the annual rate of compensation at the time of the employment was terminated.

29. No Conflicts of Interest

- A. Contractor represents and warrants that it has no actual or potential conflicts of interest in providing the requested goods or services to System Agency under this Contract or any related Solicitation and that Contractor's provision of the requested goods and/or services under this Contract and any related Solicitation will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.
- B. Contractor agrees that, if after 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.

30. Fraud, Waste, and Abuse

Contractor understands that System Agency 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. Contractor agrees to comply with all applicable laws, rules, regulations, and System Agency policies regarding fraud including, but not limited to, HHS Circular C-027.

31. Antitrust

The undersigned affirms under penalty of perjury of the laws of the State of Texas that:

- A. in connection with this Contract and any related Solicitation Response, neither I nor any representative of the Contractor has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;
- B. in connection with this Contract and any related Solicitation Response, neither I nor any representative of the Contractor has violated any federal antitrust law; and
- C. neither I nor any representative of the Contractor has directly or indirectly communicated any of the contents of this Contract and any related Solicitation Response to a competitor of the Contractor or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Contractor.

32. Legal and Regulatory Actions

Contractor 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 Contractor or any of the individuals or entities included in numbered paragraph 1 of these Contract Affirmations within the five (5) calendar years immediately preceding execution of this Contract or the submission of any related Solicitation Response that would or could impair Contractor's performance under this Contract, relate to the contracted or similar goods or services, or otherwise be relevant to System Agency's consideration of entering into this Contract. If Contractor is unable to make the preceding representation and warranty, then Contractor instead represents and warrants that it has provided to System Agency a complete, detailed disclosure of any such court or governmental agency proceeding, investigation, or other action that would or could impair Contractor's performance under this Contract, relate to the contracted or similar goods or services, or otherwise be relevant to System Agency's consideration of entering into this Contract. In addition, Contractor acknowledges this is a continuing disclosure requirement. Contractor represents and warrants that Contractor shall notify System Agency 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 System Agency shall constitute breach of contract and may result in immediate contract termination.

33. No Felony Criminal Convictions

Contractor represents that neither Contractor nor any of its employees, agents, or representatives, including any subcontractors and employees, agents, or representative of such subcontractors, have been convicted of a felony criminal offense or that if such a conviction has occurred Contractor has fully advised System Agency in writing of the facts and circumstances surrounding the convictions.

34. Unfair Business Practices

Contractor represents and warrants that it has not been the subject of allegations of Deceptive Trade Practices violations under Chapter 17 of the Texas Business and Commerce Code, or allegations of any unfair business practice in any administrative hearing or court suit and that Contractor has not been found to be liable for such practices in such proceedings. Contractor certifies that it has no officers who have served as officers of other entities who have been the subject of allegations of Deceptive Trade Practices violations or allegations of any unfair business practices in an administrative hearing or court suit and that such officers have not been found to be liable for such practices in such proceedings.

35. Entities that Boycott Israel

Pursuant to Section 2271.002 of the Texas Government Code, Contractor 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 Contractor refuses to make that certification,

Contractor shall state here any facts that make it exempt from the boycott certification:

36. E-Verify Program

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

- i. all persons employed by Contractor to perform duties within Texas; and
- ii. all persons, including subcontractors, assigned by Contractor to perform work pursuant to this Contract within the United States of America.

37. Professional or Consulting Contract

If this Contract is 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, Contractor represents and warrants that neither Contractor nor any of Contractor'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.

38. Former Agency Employees

Contractor represents and warrants, during the twelve (12) month period immediately prior to the date of the execution of this Contract, none of its employees including, but not limited to those who will provide services under the Contract, was an employee of an HHS Agency. Pursuant to Section 2252.901, Texas Government Code (relating to prohibitions regarding contracts with and involving former and retired state agency employees), Contractor will not allow any former employee of the System Agency to perform services under this Contract during the twelve (12) month period immediately following the employee's last date of employment at the System Agency.

39. Disclosure of Prior State Employment

If this Contract is for consulting services,

- A. In accordance with Section 2254.033 of the Texas Government Code, a Contractor providing consulting services 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 Contractor's offer to provide services must disclose the following information in its offer to provide services. Contractor hereby certifies that this information was provided and remains true, correct, and complete:
 - i. Name of individual(s) (Respondent or employee(s));
 - ii. Status;
 - iii. The nature of the previous employment with HHSC or the other State of Texas agency;

- iv. The date the employment was terminated and the reason for the termination; and
- v. The annual rate of compensation for the employment at the time of its termination.

B. If no information was provided in response to Section A above, Contractor certifies that neither Contractor nor any individual employed by Contractor was employed by HHSC or any other State of Texas agency at any time during the two years preceding the submission of Contractor's offer to provide services.

40. Abortion Funding Limitation

Contractor 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. Contractor represents and warrants that it is not ineligible, nor will it be ineligible during the term of this Contract, to receive appropriated funding pursuant to Article IX, Section 6.25.

41. Funding Eligibility

Contractor 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. Contractor certifies that it is not ineligible to contract with HHSC under the terms of Chapter 2272 of the Texas Government Code. If Contractor refuses to make that certification, Contractor shall state here any facts that make it exempt from the certification:

42. False Representation

Contractor understands, acknowledges, and agrees that any false representation or any failure to comply with a representation, warranty, or certification made by Contractor is subject to all civil and criminal consequences provided at law or in equity including, but not limited to, immediate termination of this Contract.

43. False Statements

Contractor represents and warrants that all statements and information prepared and submitted by Contractor in this Contract and any related Solicitation Response are current, complete, true, and accurate. Contractor acknowledges any false statement or material

misrepresentation made by Contractor during the performance of this Contract or any related Solicitation is a material breach of contract and may void this Contract. Further, Contractor understands, acknowledges, and agrees that any false representation or any failure to comply with a representation, warranty, or certification made by Contractor is subject to all civil and criminal consequences provided at law or in equity including, but not limited to, immediate termination of this Contract.

44. Permits and License

Contractor 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 this Contract.

45. Drug-Free Workplace

Contractor represents and warrants that it shall comply with the applicable provisions of the Drug-Free Work Place Act of 1988 (41 U.S.C. §701 et seq.) and maintain a drug-free work environment.

46. Equal Employment Opportunity

Contractor represents and warrants its compliance with all applicable duly enacted state and federal laws governing equal employment opportunities.

47. Federal Occupational Safety and Health Law

Contractor represents and warrants that all articles and services shall meet or exceed the safety standards established and promulgated under the Federal Occupational Safety and Health Act of 1970, as amended (29 U.S.C. Chapter 15).

48. Signature Authority

Contractor represents and warrants that the individual signing this Contract Affirmations document is authorized to sign on behalf of Contractor and to bind the Contractor.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

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

<hr/>	
Legal Name of Contractor	
<hr/>	
Assumed Business Name of Contractor, if applicable (D.B.A. or 'doing business as')	
<hr/>	
Texas County(s) for Assumed Business Name (D.B.A. or 'doing business as')	
Attach Assumed Name Certificate(s) for each County	
<hr/>	
Signature of Authorized Representative	Date Signed
<hr/>	<hr/>
Printed Name of Authorized Representative First, Middle Name or Initial, and Last Name	Title of Authorized Representative
<hr/>	<hr/>
Physical Street Address	City, State, Zip Code
<hr/>	<hr/>
Mailing Address, if different	City, State, Zip Code
<hr/>	<hr/>
Phone Number	Fax Number
<hr/>	<hr/>
Email Address	DUNS Number
<hr/>	<hr/>
Federal Employer Identification Number	Texas Payee ID No. – 11 digits
<hr/>	<hr/>
Texas Franchise Tax Number	Texas Secretary of State Filing Number
<hr/>	<hr/>

Exhibit B: 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 procedures¹.
- 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.

¹Agency 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 behalf³.

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 website⁴

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://hhs.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 C: 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.



Health and Human Services Acceptable Use Agreement (AUA) (Formerly known as the Computer Use Agreement or CUA)

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:



Health and Human Services Acceptable Use Agreement (AUA) (Formerly known as the Computer Use Agreement or CUA)

- 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) 378-9889 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 controls².

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) (Formerly 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.



Health and Human Services Acceptable Use Agreement (AUA) *(Formerly known as the Computer Use Agreement or CUA)*

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



Health and Human Services Acceptable Use Agreement (AUA) (Formerly known as the Computer Use Agreement or CUA)

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 website⁴.

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) *(Formerly 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 _____



Health and Human Services Acceptable Use Agreement (AUA) *(Formally known as the Computer Use Agreement or CUA)*

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 D: 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

GOVERNMENTAL ENTITY VERSION
HHS Data Use Agreement v.8.5 August 8, 2019

1 of 10

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

GOVERNMENTAL ENTITY VERSION
HHS Data Use Agreement v.8.5 August 8, 2019

6 of 10

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

GOVERNMENTAL ENTITY VERSION
HHS Data Use Agreement v.8.5 August 8, 2019

7 of 10

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

GOVERNMENTAL ENTITY VERSION
HHS Data Use Agreement v.8.5 August 8, 2019

8 of 10

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

To the extent permitted by the Texas Constitution, laws and rules, and without waiving any immunities or defenses available to CONTRACTOR as a governmental entity, 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) As a governmental entity, CONTRACTOR either maintains commercial insurance or self-insures with policy limits in an amount sufficient to cover CONTRACTOR's liability arising under this DUA. CONTRACTOR will either require that the policy name HHS as an additional insured or assign any payments from the insurer related to CONTRACTOR's liability arising under this DUA directly to HHS. HHSC reserves the right to consider alternative means for CONTRACTOR to satisfy

CONTRACTOR's financial responsibility under this DUA. Nothing herein shall relieve CONTRACTOR of its financial obligations set forth in this DUA if CONTRACTOR fails to maintain insurance.

(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.

Exhibit D-1: HHS System Security and Privacy Inquiry (SPI)



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

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

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

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

1. Does the applicant/bidder access, create, disclose, receive, transmit, maintain, or store Texas HHS Confidential Information in electronic systems (e.g., laptop, personal use computer, mobile device, database, server, etc.)? IF NO, STOP. THE SPI FORM IS NOT REQUIRED.	<input type="radio"/> Yes <input type="radio"/> No
2. Entity or Applicant/Bidder Legal Name	Legal Name: <input type="text"/> Legal Entity Tax Identification Number (TIN) (Last Four Numbers Only): <input type="text"/> Procurement/Contract#: <input type="text"/> Address: <input type="text"/> City: <input type="text"/> State: <input type="text"/> ZIP: <input type="text"/> Telephone #: <input type="text"/> Email Address: <input type="text"/>
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: <input type="text"/>
4. Number of Subcontractors (if Applicant/Bidder will not use subcontractors, enter "0")	Total Subcontractors: <input type="text"/>
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: <input type="text"/> Address: <input type="text"/> City: <input type="text"/> State: <input type="text"/> ZIP: <input type="text"/> Telephone #: <input type="text"/> Email Address: <input type="text"/>
	B. Privacy Official: Legal Name: <input type="text"/> Address: <input type="text"/> City: <input type="text"/> State: <input type="text"/> ZIP: <input type="text"/> Telephone #: <input type="text"/> Email Address: <input type="text"/>

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) <input type="checkbox"/> Health Insurance Portability and Accountability Act (HIPAA) data <input type="checkbox"/> Criminal Justice Information Services (CJIS) data <input type="checkbox"/> Internal Revenue Service Federal Tax Information (IRS FTI) data <input type="checkbox"/> Centers for Medicare & Medicaid Services (CMS) <input type="checkbox"/> Social Security Administration (SSA) <input type="checkbox"/> Personally Identifiable Information (PII)	<input type="checkbox"/> HIPAA	<input type="checkbox"/> CJIS	<input type="checkbox"/> IRS FTI	<input type="checkbox"/> CMS	<input type="checkbox"/> SSA	<input type="checkbox"/> 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						<input type="radio"/> a.
b. 500 to 999 individuals						<input type="radio"/> b.
c. 1,000 to 99,999 individuals						<input type="radio"/> c.
d. 100,000 individuals or more						<input type="radio"/> 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?						<input type="radio"/> Yes <input type="radio"/> 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.)						<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
<u>Action Plan for Compliance with a Timeline:</u>						<u>Compliance Date:</u>
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?						<input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A
<u>Action Plan for Compliance with a Timeline:</u>						<u>Compliance Date:</u>

<p>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?</p>	<p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A</p>
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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.</p>	<p><input type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A</p>

SECTION B: PRIVACY RISK ANALYSIS AND ASSESSMENT (To be completed by Applicant/Bidder)	
<p>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.</p>	
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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):	<input type="radio"/> Yes <input type="radio"/> No
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?	

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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.	<input type="radio"/> Yes <input type="radio"/> No

<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>3. Does Applicant/Bidder have Privacy Safeguards to protect Texas HHS Confidential Information in oral, paper and/or electronic form?</p> <p>"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 164.330), 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.</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>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?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>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?</p>	<p><input type="radio"/> Yes</p> <p><input type="radio"/> No</p>
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

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 <input type="checkbox"/>
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.	
<p>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?</p> <ul style="list-style-type: none"> 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 <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<p><input type="radio"/> Yes <input type="radio"/> No</p>
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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)?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
<p>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.</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p>	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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).	<input type="radio"/> Yes <input type="radio"/> No
<p><i>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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to:</i> http://csrc.nist.gov/publications/fips </p>	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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.)	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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.)?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>


<p>10. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information that is <u>transmitted</u> over a public network (e.g., the Internet, WiFi, etc.)?</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>11. Does Applicant/Bidder use encryption products to protect Texas HHS Confidential Information <u>stored</u> on end user devices (e.g., laptops, USBs, tablets, smartphones, external hard drives, desktops, etc.)?</p> <p>If yes, upon request must provide evidence such as a screen shot or a system report.</p> <p><i>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.</i></p> <p><i>For more information regarding FIPS 140-2 encryption products, please refer to: http://csrc.nist.gov/publications/fips</i></p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>13. Is Applicant/Bidder willing to perform or submit to a criminal background check on Authorized Users?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>
<p>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?</p>	<input type="radio"/> Yes <input type="radio"/> No
<p><u>Action Plan for Compliance with a Timeline:</u></p>	<p><u>Compliance Date:</u></p>

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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>
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?	<input type="radio"/> Yes <input type="radio"/> No
<i>For more information regarding TGC, Section 2054.516 DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS, please refer to: https://legiscon.com/TX/text/H88/2017</i>	
<u>Action Plan for Compliance with a Timeline:</u>	<u>Compliance Date:</u>

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: <input type="checkbox"/> DFPS: <input type="checkbox"/> DSHS: <input type="checkbox"/>	Requesting Department(s):
--	---------------------------

Legal Entity Tax Identification Number (TIN) (Last four Only): <table border="1"><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>											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 8. 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 332.

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 individual. 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 offshore their data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<https://portal.msrc.microsoft.com/en-us/>

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

<https://docs.microsoft.com/en-us/windows/security/threat-protection/>

Item #17. Answer "Yes" if your business reviews system security logs on computing systems that access or store Texas HHS Confidential Information for abnormal activity or security concerns on a regular basis. If you use a Microsoft Windows system, refer to the Microsoft website for ensuring your system is logging security events, see example:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies>

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

Item #19. Answer "Yes" if your business ensures that all public facing websites and mobile applications containing HHS Confidential Information meet security testing standards set forth within the Texas Government Code (TGC), Section 2054.316

SECTION D. SIGNATURE AND SUBMISSION

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

Exhibit E: Experience Reference Form

Exhibit E

IT Organizational Maturity Assessment – 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 IT Organizational Maturity Assessment 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:			

Exhibit E-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 F: 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
D.1.1	A 5-level organizational model	
D1.2	A comprehensive and documented assessment methodology	
D1.3	A list of participants for the survey(s) and interviews	
D1.4	Communication Plan and Escalation Policy	
D1.5	A completed survey summary to evaluate and benchmark the current organizational maturity	
D1.6	Validation interview and focus group recorded results	
D1.7	A summary of items reviewed in archive review process	
D1.8	Milestone Closeout	
	Total	\$

Deliverable No.	Deliverable	Deliverable Cost
D2.1	A list of HHSC's IT organizational strengths and weaknesses in terms of IT processes and practices	
D2.2	Identified "success drivers"	
D2.3	A roadmap for organizational improvement	
D2.4	Organizational change management tools, communications, plans to aid in the implementation of recommendations	
D2.5	Documented current level of organizational maturity	
D2.6	Milestone closeout	
	Total	\$

Deliverable No.	Deliverable	Deliverable Cost
D3.1	Findings	
D3.2	Recommendations	
D3.3	Milestone Closeout	
	Total	\$

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

Exhibit G: HHSC Uniform Terms and Conditions



TEXAS

Health and Human Services

Health and Human Services (HHS)

Uniform Terms and Conditions - Vendor

Version 3.0

Published and Effective - November 7, 2019

Responsible Office: Chief Counsel

Table of Contents

ARTICLE I. DEFINITIONS AND INTERPRETIVE PROVISIONS	5
1.1 DEFINITIONS	5
1.2 INTERPRETIVE PROVISIONS	7
ARTICLE II. PAYMENT PROVISIONS	8
2.1 PROMPT PAYMENT	8
2.2 ANCILLARY AND TRAVEL EXPENSES	8
2.3 NO QUANTITY GUARANTEES	8
2.4 TAXES	8
ARTICLE III. STATE AND FEDERAL FUNDING	8
3.1 EXCESS OBLIGATIONS PROHIBITED	8
3.2 NO DEBT AGAINST THE STATE	8
3.3 DEBT AND DELINQUENCIES.....	9
3.4 REFUNDS AND OVERPAYMENTS	9
ARTICLE IV. WARRANTY, AFFIRMATIONS, ASSURANCES, AND CERTIFICATIONS.....	9
4.1 WARRANTY.....	9
4.2 GENERAL AFFIRMATIONS	9
4.3 FEDERAL ASSURANCES	10
4.4 FEDERAL CERTIFICATIONS	10
ARTICLE V. INTELLECTUAL PROPERTY.....	10
5.1 OWNERSHIP OF WORK PRODUCT	10
5.2 CONTRACTOR'S PRE-EXISTING WORKS.....	10
5.3 THIRD PARTY IP.....	11
5.4 AGREEMENTS WITH EMPLOYEES AND SUBCONTRACTORS	11
5.5 DELIVERY UPON TERMINATION OR EXPIRATION	11
5.6 SURVIVAL.....	11
5.7 SYSTEM AGENCY DATA.....	12
ARTICLE VI. PROPERTY	12
6.1 USE OF STATE PROPERTY	12
6.2 DAMAGE TO GOVERNMENT PROPERTY.....	13
6.3 PROPERTY RIGHTS UPON TERMINATION OR EXPIRATION OF CONTRACT.....	13
ARTICLE VII. WORK ORDERS.....	13
7.1 WORK ORDERS.....	13

7.2	PROPOSALS	13
7.3	RESPONSIBILITY	13
7.4	TERMINATION.....	13
ARTICLE VIII RECORD RETENTION, AUDIT, AND CONFIDENTIALITY		13
8.1	RECORD MAINTENANCE AND RETENTION	13
8.2	AGENCY’S RIGHT TO AUDIT	14
8.3	RESPONSE/COMPLIANCE WITH AUDIT OR INSPECTION FINDINGS	14
8.4	STATE AUDITOR’S RIGHT TO AUDIT	15
8.5	CONFIDENTIALITY.....	15
ARTICLE IX. CONTRACT REMEDIES AND EARLY TERMINATION		15
9.1	CONTRACT REMEDIES.....	15
9.2	TERMINATION FOR CONVENIENCE	15
9.3	TERMINATION FOR CAUSE	16
9.4	CONTRACTOR RESPONSIBILITY FOR SYSTEM AGENCY’S TERMINATION COSTS	16
ARTICLE X. INDEMNITY.....		16
10.1	GENERAL INDEMNITY	16
10.2	INTELLECTUAL PROPERTY	17
10.3	ADDITIONAL INDEMNITY PROVISIONS	17
ARTICLE XI. GENERAL PROVISIONS		18
11.1	AMENDMENT	18
11.2	INSURANCE	18
11.3	LIMITATION ON AUTHORITY.....	18
11.4	LEGAL OBLIGATIONS.....	18
11.5	CHANGE IN LAWS AND COMPLIANCE WITH LAWS.....	19
11.6	E-VERIFY PROGRAM.....	19
11.7	PERMITTING AND LICENSURE.....	19
11.8	SUBCONTRACTORS	19
11.9	INDEPENDENT CONTRACTOR.....	19
11.10	GOVERNING LAW AND VENUE	20
11.11	SEVERABILITY	20
11.12	SURVIVABILITY.....	20
11.13	FORCE MAJEURE.....	20
11.14	DISPUTE RESOLUTION.....	20
11.15	NO IMPLIED WAIVER OF PROVISIONS	21

11.16	MEDIA RELEASES	21
11.17	NO MARKETING ACTIVITIES	21
11.18	PROHIBITION ON NON-COMPETE RESTRICTIONS	21
11.19	SOVEREIGN IMMUNITY	22
11.20	ENTIRE CONTRACT AND MODIFICATION	22
11.21	COUNTERPARTS	22
11.22	CIVIL RIGHTS	22
11.23	ENTERPRISE INFORMATION MANAGEMENT STANDARDS	23
11.24	DISCLOSURE OF LITIGATION	23
11.25	NO THIRD-PARTY BENEFICIARIES	24
11.26	BINDING EFFECT	24

ARTICLE I. DEFINITIONS AND INTERPRETIVE PROVISIONS

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, which documents changes to the Contract other than those permitted by Work Orders.

“Attachment” means documents, terms, conditions, or information added to this Contract following the Signature Document or included by reference and made a part of this Contract.

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

“Contractor” means the Party selected to provide the goods or Services to the State under this Contract.

“Deliverable” means a Work Product(s), including all reports and project documentation, 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.

“Goods” means supplies, materials, or equipment.

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

“Health and Human Services” or “HHS” includes the Department of State Health Services (DSHS), in addition to the Health and Human Services Commission.

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

“Intellectual Property Rights” means the worldwide proprietary rights or interests, including patent, copyright, trade secret, and trademark rights, as such rights may be evidenced by or embodied in:

- i. any idea, design, concept, personality right, method, process, technique, apparatus, invention, discovery, or improvement;

- ii. any work of authorship, including any compilation, computer code, website or web page design, literary work, pictorial work, or graphic work;
- iii. any trademark, service mark, trade dress, trade name, branding, or other indicia of source or origin;
- iv. domain name registrations; and
- v. any other proprietary or similar rights. The Intellectual Property Rights of a Party include all worldwide proprietary rights or interests that the Party may have acquired by assignment, by exclusive license, or by license with the right to grant sublicenses.

“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.

“Scope of Work” means the description of Services and Deliverables specified in the Contract and 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 (including any published addenda, exhibits, and Attachments) under which the goods or Services provided under the Contract were initially requested, which is incorporated by reference for all purposes in its entirety.

“Solicitation Response” means Contractor’s full and complete response (including any Attachments and addenda) to the Solicitation, which is incorporated by reference for all purposes in its entirety.

“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 the State Travel Management Program through the Texas Comptroller of Public Accounts website and 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, authorized representatives, and designees of those agencies. These agencies include: HHSC and the Department of State Health Services.

“Third Party IP” means the Intellectual Property Rights of any third party that is not a party to this Contract, and that is not a Subcontractor.

“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.

“Work Product” means any and all works, including work papers, notes, materials, approaches, designs, specifications, systems, innovations, improvements, inventions, software, programs, source code, documentation, training materials, audio or audiovisual recordings, methodologies, concepts, studies, reports, whether finished or unfinished, and whether or not included in the Deliverables, that are developed, produced, generated, or provided by Contractor in connection with Contractor’s performance of its duties under the Contract or through use of any funding provided under this Contract.

1.2 INTERPRETIVE PROVISIONS

- A. The meanings of defined terms include the singular and plural forms.
- 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, 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, 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. PAYMENT PROVISIONS

2.1 PROMPT PAYMENT

Payment shall be made in accordance with Chapter 2251 of the Texas Government Code, commonly known as the Texas Prompt Payment Act. Chapter 2251 of the Texas Government Code shall govern remittance of payment and remedies for late payment and non-payment.

2.2 ANCILLARY AND TRAVEL EXPENSES

- A. 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.
- B. 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* available at the Texas Comptroller of Public Accounts State Travel Management Program website.

2.3 NO QUANTITY GUARANTEES

The System Agency makes no guarantee of volume or usage of work under this Contract. All Work requested may be on an irregular and as needed basis throughout the Contract term.

2.4 TAXES

Purchases made for State of Texas use are exempt from the State Sales Tax and Federal Excise Tax. Contractor represents and warrants that it shall pay all taxes or similar amounts resulting from the Contract, including, but not limited to, any federal, State, or local income, sales or excise taxes of Contractor or its employees. System Agency shall not be liable for any taxes resulting from the contract.

ARTICLE III. STATE AND FEDERAL FUNDING

3.1 EXCESS OBLIGATIONS PROHIBITED

The Contract is subject to termination or cancellation, without penalty to the System Agency, either in whole or in part, subject to the availability of state funds. System Agency is a state agency whose authority and appropriations are subject to actions of the Texas Legislature. If System Agency becomes subject to a legislative change, revocation of statutory authority, or lack of appropriated funds that would render either System Agency's or Contractor's delivery or performance under the Contract impossible or unnecessary, the Contract will be terminated or cancelled and be deemed null and void. In the event of a termination or cancellation under this Section, System Agency will not be liable to Contractor for any damages that are caused or associated with such termination, or cancellation, and System Agency will not be required to give prior notice.

3.2 NO DEBT AGAINST THE STATE

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

3.3 DEBT AND DELINQUENCIES

Contractor agrees that any payments due under the Contract shall be directly applied towards eliminating any debt or delinquency it has to the State of Texas including, but not limited to, delinquent taxes, delinquent student loan payments, and delinquent child support.

3.4 REFUNDS AND OVERPAYMENTS

- A. At its sole discretion, the System Agency may:
- i. withhold all or part of any payments to Contractor to offset overpayments, unallowable or ineligible costs made to the Contractor, or if any required financial status report(s) is not submitted by the due date(s); or,
 - ii. require Contractor to promptly refund or credit - within thirty (30) calendar days of written notice - any funds erroneously paid by System Agency which are not expressly authorized under the Contract.
- B. "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 shall 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 shall be completed in a manner consistent with standards under the terms of this Contract, in the applicable trade, profession, or industry; shall conform to or exceed the specifications set forth in the Contract; and all Deliverables shall be fit for ordinary use, of good quality, and with no material defects. If System Agency, in its sole discretion, determines Contractor has failed 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:

- i. Repair or replace all defective or damaged Work;
- ii. Refund any payment Contractor received from System Agency for all defective or damaged Work and, in conjunction therewith, require Contractor to accept the return of such Work; and,
- iii. Take necessary action to ensure that Contractor's future performance and Work conform to the Contract requirements.

4.2 GENERAL AFFIRMATIONS

Contractor certifies that, to the extent General Affirmations are incorporated into the Contract under the Signature Document, the Contractor has reviewed the General Affirmations and that Contractor is in compliance with all requirements.

4.3 FEDERAL ASSURANCES

Contractor certifies that, to the extent federal assurances are incorporated into the Contract under the Signature Document, the Contractor has reviewed the federal assurances and that Contractor is in compliance with all requirements.

4.4 FEDERAL CERTIFICATIONS

Contractor certifies that, to the extent federal certifications are incorporated into the Contract under the Signature Document, the Contractor has reviewed the federal certifications and that Contractor is in compliance with all requirements. In addition, Contractor certifies that it is and shall remain in compliance with all applicable federal laws, rules, and regulations, as they may pertain to this Contract.

ARTICLE V. INTELLECTUAL PROPERTY

5.1 OWNERSHIP OF WORK PRODUCT

- A. All right, title, and interest in the Work Product, including all Intellectual Property Rights therein, is exclusively owned by System Agency. Contractor and Contractor's employees will have no rights in or ownership of the Work Product or any other property of System Agency.
- B. Any and all Work Product that is copyrightable under United States copyright law is deemed to be "work made for hire" owned by System Agency, as provided by Title 17 of the United States Code. To the extent that Work Product does not qualify as a "work made for hire" under applicable federal law, Contractor hereby irrevocably assigns and transfers to System Agency, its successors and assigns, the entire right, title, and interest in and to the Work Product, including any and all Intellectual Property Rights embodied therein or associated therewith, and in and to all works based upon, derived from, or incorporating the Work Product, and in and to all income, royalties, damages, claims and payments now or hereafter due or payable with respect thereto, and in and to all causes of action, either in law or in equity for past, present or future infringement based on the copyrights, and in and to all rights corresponding to the foregoing.
- C. Contractor agrees to execute all papers and to perform such other acts as System Agency may deem necessary to secure for System Agency or its designee the rights herein assigned.
- D. In the event that Contractor has any rights in and to the Work Product that cannot be assigned to System Agency, Contractor hereby grants to System Agency an exclusive, worldwide, royalty-free, transferable, irrevocable, and perpetual license, with the right to sublicense, to reproduce, distribute, modify, create derivative works of, publicly perform and publicly display, make, have made, use, sell and offer for sale the Work Product and any products developed by practicing such rights.
- E. The foregoing does not apply to Incorporated Pre-existing Works or Third Party IP that are incorporated in the Work Product by Contractor. Contractor shall provide System Agency access during normal business hours to all Vendor materials, premises, and computer files containing the Work Product.

5.2 CONTRACTOR'S PRE-EXISTING WORKS

- A. To the extent that Contractor incorporates into the Work Product any works of Contractor that were created by Contractor or that Contractor acquired rights in prior to the Effective

Date of this Contract (“**Incorporated Pre-existing Works**”), Contractor retains ownership of such Incorporated Pre-existing Works.

- B. Contractor hereby grants to System Agency an irrevocable, perpetual, non-exclusive, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, modify, copy, create derivative works of, publish, publicly perform and display, sell, offer to sell, make and have made, the Incorporated Pre-existing Works, in any medium, with or without the associated Work Product.
- C. Contractor represents, warrants, and covenants to System Agency that Contractor has all necessary right and authority to grant the foregoing license in the Incorporated Pre-existing Works to System Agency.

5.3 THIRD PARTY IP

- A. To the extent that any Third Party IP is included or incorporated in the Work Product by Contractor, Contractor hereby grants to System Agency, or shall obtain from the applicable third party for System Agency’s benefit, the irrevocable, perpetual, non-exclusive, worldwide, royalty-free right and license, for System Agency’s internal business purposes only,
 - i. to use, reproduce, display, perform, distribute copies of, and prepare derivative works based upon such Third Party IP and any derivative works thereof embodied in or delivered to System Agency in conjunction with the Work Product, and
 - ii. to authorize others to do any or all of the foregoing.
- B. Contractor shall obtain System Agency’s advance written approval prior to incorporating any Third Party IP into the Work Product, and Contractor shall notify System Agency on delivery of the Work Product if such materials include any Third Party IP.
- C. Contractor shall provide System Agency all supporting documentation demonstrating Contractor’s compliance with this **Section 5.3**, including without limitation documentation indicating a third party’s written approval for Contractor to use any Third Party IP that may be incorporated in the Work Product.

5.4 AGREEMENTS WITH EMPLOYEES AND SUBCONTRACTORS

Contractor shall have written, binding agreements with its employees and subcontractors that include provisions sufficient to give effect to and enable Contractor’s compliance with Contractor’s obligations under this **Article V**.

5.5 DELIVERY UPON TERMINATION OR EXPIRATION

No later than the first calendar day after the termination or expiration of the Contract or upon System Agency’s request, Contractor shall deliver to System Agency all completed, or partially completed, Work Product, including any Incorporated Pre-existing Works, and any and all versions thereof. Contractor’s failure to timely deliver such Work Product is a material breach of the Contract. Contractor will not retain any copies of the Work Product or any documentation or other products or results of Contractor’s activities under the Contract without the prior written consent of System Agency.

5.6 SURVIVAL

The provisions and obligations of this **Article V** survive any termination or expiration of the Contract.

5.7 SYSTEM AGENCY DATA

- A. As between the Parties, all data and information acquired, accessed, or made available to Contractor by, through, or on behalf of System Agency or System Agency contractors, including all electronic data generated, processed, transmitted, or stored by Contractor in the course of providing data processing services in connection with Contractor's performance hereunder (the "System Agency Data"), is owned solely by System Agency.
- B. Contractor has no right or license to use, analyze, aggregate, transmit, create derivatives of, copy, disclose, or process the System Agency Data except as required for Contractor to fulfill its obligations under the Contract or as authorized in advance in writing by System Agency.
- C. For the avoidance of doubt, Contractor is expressly prohibited from using, and from permitting any third party to use, System Agency Data for marketing, research, or other non-governmental or commercial purposes, without the prior written consent of System Agency.
- D. Contractor shall make System Agency Data available to System Agency, including to System Agency's designated vendors, as directed in writing by System Agency. The foregoing shall be at no cost to System Agency.
- E. Furthermore, the proprietary nature of Contractor's systems that process, store, collect, and/or transmit the System Agency Data shall not excuse Contractor's performance of its obligations hereunder.

ARTICLE VI. PROPERTY

6.1 USE OF STATE PROPERTY

- A. Contractor is prohibited from using State Property for any purpose other than performing Services authorized under the Contract.
- B. State Property includes, but is not limited to, System Agency's office space, identification badges, System Agency information technology equipment and networks (e.g., laptops, portable printers, cell phones, iPads or tablets, external hard drives, data storage devices, any System Agency-issued software, and the System Agency Virtual Private Network (VPN client)), and any other resources of System Agency.
- C. Contractor shall not remove State Property from the continental United States. In addition, Contractor may not use any computing device to access System Agency's network or e-mail while outside of the continental United States.
- D. Contractor shall not perform any maintenance services on State Property unless the Contract expressly authorizes such Services.
- E. During the time that State Property is in the possession of Contractor, Contractor shall be responsible for:
 - i. all repair and replacement charges incurred by State Agency that are associated with loss of State Property or damage beyond normal wear and tear, and
 - ii. all charges attributable to Contractor's use of State Property that exceeds the Contract scope. Contractor shall fully reimburse such charges to System Agency within ten (10) calendar days of Contractor's receipt of System Agency's notice of amount due. Use of State Property for a purpose not authorized by the Contract shall constitute breach of contract and may result in termination of the Contract and the pursuit of other remedies available to System Agency under contract, at law, or in equity.

6.2 DAMAGE TO GOVERNMENT PROPERTY

- A. In the event of loss, destruction, or damage to any System Agency or State of Texas owned, leased, or occupied property or equipment by Contractor or Contractor's employees, agents, Subcontractors, and suppliers, Contractor shall be liable to System Agency and the State of Texas for the full cost of repair, reconstruction, or replacement of the lost, destroyed, or damaged property.
- B. Contractor shall notify System Agency of the loss, destruction, or damage of equipment or property within one (1) business day. Contractor shall reimburse System Agency and the State of Texas for such property damage within 10 calendar days after Contractor's receipt of System Agency's notice of amount due.

6.3 PROPERTY RIGHTS UPON TERMINATION OR EXPIRATION OF CONTRACT

In the event the Contract is terminated for any reason, or upon its expiration State Property remains the property of the System Agency and must be returned to the System Agency by the end date of the Contract or upon System Agency's request.

ARTICLE VII. WORK ORDERS

7.1 WORK ORDERS

If the Contract is for indefinite quantities of Services, as specified in the Signature Document, all Work will be performed in accordance with properly executed Work Orders.

7.2 PROPOSALS

For Work Order contracts, the Contractor shall submit to System Agency separate proposals, including pricing and a project plan, for each Project.

7.3 RESPONSIBILITY

For each approved Project, the Contractor shall be responsible for all Work assigned under the Work Order. 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 any other information or special conditions as may be necessary for the Work assigned.

7.4 TERMINATION

If this Work Order is in effect on the day the Contract would otherwise expire, the Contract will remain in effect until this Work Order is terminated or expires; and the Contract and this Work Order may be amended after such termination or expiration to extend the performance period or add ancillary deliverables or services, only to the extent necessary.

ARTICLE VIII. RECORD RETENTION, AUDIT, AND CONFIDENTIALITY

8.1 RECORD MAINTENANCE AND RETENTION

- A. Contractor shall 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.

- B. Contractor shall maintain and retain legible copies of this Contract and all records relating to the performance of the Contract including supporting fiscal documents adequate to ensure that claims for contract funds are in accordance with applicable State of Texas requirements. These records shall be maintained and retained by Contractor for a minimum of seven (7) years after the Contract expiration date or seven (7) years after the completion of all audit, claim, litigation, or dispute matters involving the Contract are resolved, whichever is later.

8.2 AGENCY'S RIGHT TO AUDIT

- A. Contractor shall make available at reasonable times and upon reasonable notice, and for reasonable periods, work papers, reports, books, records, supporting documents kept current by Contractor pertaining to the Contract for purposes of inspecting, monitoring, auditing, or evaluating by System Agency and the State of Texas.
- B. In addition to any right of access arising by operation of law, Contractor and any of Contractor's affiliate or subsidiary organizations, or Subcontractors shall 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 shall 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 shall 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.
- C. If deemed necessary by the System Agency or any duly authorized authority, for the purpose of investigation or hearing, Contractor shall produce original documents related to this Contract.
- D. The System Agency and any duly authorized authority shall have the right to audit billings both before and after payment, and all documentation that substantiates the billings.
- E. Contractor shall include this provision concerning the right of access to, and examination of, sites and information related to this Contract in any Subcontract it awards.

8.3 RESPONSE/COMPLIANCE WITH AUDIT OR INSPECTION FINDINGS

- A. Contractor must act to ensure its and its Subcontractors' 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 Services and Deliverables provided. Any such correction will be at Contractor's or its Subcontractor's sole expense. Whether Contractor's action corrects the noncompliance shall be solely the decision of the System Agency.

- B. As part of the Services, Contractor must provide to System Agency 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.

8.4 STATE AUDITOR'S RIGHT TO AUDIT

- A. The state auditor may conduct an audit or investigation of any entity receiving funds from the state directly under the Contract or indirectly through a subcontract under the Contract. The 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, under the direction of the legislative audit committee, 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 state auditor must provide the state auditor with access to any information the state auditor considers relevant to the investigation or audit.
- B. The Contractor shall comply with any rules and procedures of the state auditor in the implementation and enforcement of Section 2262.154 of the Texas Government Code.

8.5 CONFIDENTIALITY

Contractor shall maintain as confidential and shall not disclose to third parties without System Agency's prior written consent, any System Agency information including but not limited to System Agency Data, System Agency's business activities, practices, systems, conditions and services. This section will survive termination or expiration of this Contract. The obligations of Contractor under this section will survive termination or expiration of this Contract. This requirement must be included in all subcontracts awarded by Contractor.

ARTICLE IX. CONTRACT REMEDIES AND EARLY TERMINATION

9.1 CONTRACT REMEDIES

To ensure Contractor's full performance of the Contract and compliance with applicable law, the System Agency reserves the right to hold Contractor accountable for breach of contract or substandard performance and may take remedial or corrective actions, including, but not limited to:

- i. suspending all or part of the Contract;
- ii. requiring the Contractor to take specific actions in order to remain in compliance with the Contract;
- iii. recouping payments made by the System Agency to the Contractor found to be in error;
- iv. suspending, limiting, or placing conditions on the Contractor's continued performance of Work; or
- v. imposing any other remedies, sanctions, or penalties authorized under this Contract or permitted by federal or state law.

9.2 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 the System Agency's notice of termination.

9.3 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:

i. Material Breach

The System Agency will have the right to terminate the Contract in whole or in part if the System Agency determines, in 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 System for Award Management (SAM) will also constitute a material breach of the Contract.

ii. 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 Work, or otherwise fully perform its responsibilities under the Contract.

9.4 CONTRACTOR RESPONSIBILITY FOR SYSTEM AGENCY'S TERMINATION COSTS

If the System Agency terminates the Contract for cause, the Contractor shall 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 attributable to Contractor's failure to perform any Work in accordance with the terms of the Contract.

ARTICLE X. INDEMNITY

10.1 GENERAL INDEMNITY

- A. CONTRACTOR SHALL DEFEND, INDEMNIFY AND HOLD HARMLESS THE STATE OF TEXAS AND SYSTEM AGENCY, AND/OR THEIR OFFICERS, AGENTS, EMPLOYEES, REPRESENTATIVES, CONTRACTORS, ASSIGNEES, AND/OR DESIGNEES FROM ANY AND ALL LIABILITY, ACTIONS, CLAIMS, DEMANDS, OR SUITS, AND ALL RELATED COSTS, ATTORNEY FEES, AND EXPENSES ARISING OUT OF OR RESULTING FROM ANY ACTS OR OMISSIONS OF CONTRACTOR OR ITS AGENTS, EMPLOYEES, SUBCONTRACTORS, ORDER FULFILLERS, OR SUPPLIERS OF SUBCONTRACTORS IN THE EXECUTION OR PERFORMANCE OF THE CONTRACT AND ANY PURCHASE ORDERS ISSUED UNDER THE CONTRACT.**
- B. 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 FROM THE NEGLIGENT ACTS OF OMISSIONS OF THE SYSTEM AGENCY OR ITS EMPLOYEES.

- C. For the avoidance of doubt, System Agency shall not indemnify Contractor or any other entity under the Contract.

10.2 INTELLECTUAL PROPERTY

CONTRACTOR SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS THE SYSTEM AGENCY AND THE STATE OF TEXAS FROM AND AGAINST ANY AND ALL CLAIMS, VIOLATIONS, MISAPPROPRIATIONS, OR INFRINGEMENT OF ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET, OR OTHER INTELLECTUAL PROPERTY RIGHTS AND/OR OTHER INTANGIBLE PROPERTY, PUBLICITY OR PRIVACY RIGHTS, AND/OR IN CONNECTION WITH OR ARISING FROM:

- i. THE PERFORMANCE OR ACTIONS OF CONTRACTOR PURSUANT TO THIS CONTRACT;
- ii. ANY DELIVERABLE, WORK PRODUCT, CONFIGURED SERVICE OR OTHER SERVICE PROVIDED HEREUNDER; AND/OR
- iii. SYSTEM AGENCY'S AND/OR CONTRACTOR'S USE OF OR ACQUISITION OF ANY REQUESTED SERVICES OR OTHER ITEMS PROVIDED TO SYSTEM AGENCY BY CONTRACTOR OR OTHERWISE TO WHICH SYSTEM AGENCY HAS ACCESS AS A RESULT OF CONTRACTOR'S PERFORMANCE UNDER THE CONTRACT.

10.3 ADDITIONAL INDEMNITY PROVISIONS

- A. CONTRACTOR AND SYSTEM AGENCY AGREE TO FURNISH TIMELY WRITTEN NOTICE TO EACH OTHER OF ANY INDEMNITY CLAIM. CONTRACTOR SHALL BE LIABLE TO PAY ALL COSTS OF DEFENSE, INCLUDING ATTORNEYS' FEES.
- B. THE DEFENSE SHALL BE COORDINATED BY THE CONTRACTOR WITH THE OFFICE OF THE TEXAS ATTORNEY GENERAL WHEN TEXAS STATE AGENCIES ARE NAMED DEFENDANTS IN ANY LAWSUIT AND CONTRACTOR MAY NOT AGREE TO ANY SETTLEMENT WITHOUT FIRST OBTAINING THE CONCURRENCE FROM THE OFFICE OF THE TEXAS ATTORNEY GENERAL.
- C. CONTRACTOR SHALL REIMBURSE SYSTEM AGENCY AND THE STATE OF TEXAS FOR ANY CLAIMS, DAMAGES, COSTS, EXPENSES OR OTHER AMOUNTS, INCLUDING, BUT NOT LIMITED TO, ATTORNEYS' FEES AND COURT COSTS, ARISING FROM ANY SUCH CLAIM. IF THE SYSTEM AGENCY DETERMINES THAT A CONFLICT EXISTS BETWEEN ITS INTERESTS AND THOSE OF CONTRACTOR OR IF SYSTEM AGENCY IS REQUIRED BY APPLICABLE LAW TO SELECT SEPARATE COUNSEL, SYSTEM AGENCY WILL BE PERMITTED TO SELECT SEPARATE COUNSEL AND CONTRACTOR SHALL PAY ALL REASONABLE COSTS OF SYSTEM AGENCY'S COUNSEL.

ARTICLE XI. GENERAL PROVISIONS

11.1 AMENDMENT

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

11.2 INSURANCE

- A. Unless otherwise specified in this Contract, Contractor shall 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 shall 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 shall 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.
- B. 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.

11.3 LIMITATION ON AUTHORITY

- A. The authority granted to Contractor by the System Agency is limited to the terms of the Contract.
- B. Contractor shall not have any authority to act for or on behalf of the System Agency or the State of Texas except as expressly provided for in the Contract; no other authority, power, or use is granted or implied. Contractor may not incur any debt, obligation, expense, or liability of any kind on behalf of System Agency or the State of Texas.
- C. Contractor may not rely upon implied authority and is not granted authority under the Contract to:
 - i. Make public policy on behalf of the System Agency;
 - ii. Promulgate, amend, or disregard administrative regulations or program policy decisions made by State and federal agencies responsible for administration of a System Agency program; or
 - iii. Unilaterally communicate or negotiate with any federal or state agency or the Texas Legislature on behalf of the System Agency regarding System Agency programs or the Contract. However, upon System Agency request and with reasonable notice from System Agency to the Contractor, the Contractor shall assist the System Agency in communications and negotiations regarding the Work under the Contract with state and federal governments.

11.4 LEGAL OBLIGATIONS

Contractor shall 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 shall be deemed to have knowledge of all applicable laws and regulations and be deemed to understand them.

11.5 CHANGE IN LAWS AND COMPLIANCE WITH LAWS

Contractor shall comply with all laws, regulations, requirements and guidelines applicable to a vendor providing services and products required by the Contract to the State of Texas, as these laws, regulations, requirements and guidelines currently exist and as amended throughout the term of the Contract. System Agency reserves the right, in its sole discretion, to unilaterally amend the Contract to incorporate any modifications necessary for System Agency's compliance, as an agency of the State of Texas, with all applicable state and federal laws, regulations, requirements and guidelines.

11.6 E-VERIFY PROGRAM

Contractor certifies that for Contracts for Services, Contractor shall utilize the U.S. Department of Homeland Security's E-Verify system during the term of the Contract to determine the eligibility of:

- i. all persons employed by Contractor to perform duties within Texas; and
- ii. all persons, including subcontractors, assigned by the Contractor to perform Work pursuant to the Contract within the United States of America.

11.7 PERMITTING AND LICENSURE

At Contractor's sole expense, Contractor shall 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 shall be responsible for payment of all taxes, assessments, fees, premiums, permits, and licenses required by law. Contractor shall be responsible for payment of any such government obligations not paid by its Subcontractors during performance of this Contract.

11.8 SUBCONTRACTORS

Contractor may not subcontract any or all of the Work and/or obligations under the Contract without prior written approval of the System Agency. Subcontracts, if any, entered into by the Contractor shall be in writing and be subject to the requirements of the Contract. Should Contractor Subcontract any of the services required in the Contract, Contractor expressly understands and acknowledges that in entering into such Subcontract(s), System Agency is in no manner liable to any subcontractor(s) of Contractor. In no event shall this provision relieve Contractor of the responsibility for ensuring that the services performed under all Subcontracts are rendered in compliance with the Contract.

11.9 INDEPENDENT CONTRACTOR

Contractor and Contractor's employees, representatives, agents, Subcontractors, suppliers, and third-party service providers shall serve as independent contractors in providing the services under the Contract. Neither Contractor nor System Agency is an agent of the other and neither may make any commitments on the other party's behalf. Contractor shall have no claim against System Agency for vacation pay, sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee

benefits of any kind. The Contract shall not create any joint venture, partnership, agency, or employment relationship between Contractor and System Agency.

11.10 GOVERNING LAW AND VENUE

This Contract shall be governed by and construed in accordance with the laws of the State of Texas, without regard to the conflicts of law provisions. The venue of any suit arising under the Contract is fixed in any court of competent jurisdiction of Travis County, Texas, unless the specific venue is otherwise identified in a statute which directly names or otherwise identifies its applicability to the System Agency.

11.11 SEVERABILITY

If any provision of the Contract is held to be illegal, invalid or unenforceable by a court of law or equity, such construction will not affect the legality, validity or enforceability of any other provision or provisions of this Contract. It is the intent and agreement of the Parties this Contract shall be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting another provision that is valid, legal and enforceable and that achieves the same objective. All other provisions of this Contract will continue in full force and effect.

11.12 SURVIVABILITY

Expiration or termination of the Contract for any reason does not release Contractor from any liability or obligation set forth in the Contract that is expressly stated to survive any such expiration or termination, that by its nature would be intended to be applicable following any such expiration or termination, or that is necessary to fulfill the essential purpose of the Contract, including without limitation the provisions regarding warranty, indemnification, confidentiality, and rights and remedies upon termination.

11.13 FORCE MAJEURE

Neither Contractor nor System Agency shall be liable to the other for any delay in, or failure of performance of, any requirement included in the Contract caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either party and that by exercise of due foresight such party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such party is unable to overcome.

11.14 DISPUTE RESOLUTION

- A. The dispute resolution process provided for in Chapter 2260 of the Texas Government Code must be used to attempt to resolve any dispute arising under the Contract. If the Contractor's claim for breach of contract cannot be resolved informally with the System Agency, the claim shall be submitted to the negotiation process provided in Chapter 2260. To initiate the process, the Contractor shall submit written notice, as required by Chapter 2260, to the individual identified in the Contract for receipt of notices. Any informal resolution efforts shall in no way modify the requirements or toll the timing of the formal written notice of a claim for breach of contract required under §2260.051 of the Texas

Government Code. Compliance by the Contractor with Chapter 2260 is a condition precedent to the filing of a contested case proceeding under Chapter 2260.

- B. The contested case process provided in Chapter 2260 is the Contractor's sole and exclusive process for seeking a remedy for an alleged breach of contract by the System Agency if the Parties are unable to resolve their disputes as described above.
- C. Notwithstanding any other provision of the Contract to the contrary, unless otherwise requested or approved in writing by the System Agency, the Contractor shall continue performance and shall not be excused from performance during the period of any breach of contract claim or while the dispute is pending. However, the Contractor may suspend performance during the pendency of such claim or dispute if the Contractor has complied with all provisions of Section 2251.051, Texas Government Code, and such suspension of performance is expressly applicable and authorized under that law.

11.15 NO IMPLIED WAIVER OF PROVISIONS

The failure of the System Agency to object to or to take affirmative action with respect to any conduct of the Contractor which is in violation or breach of the terms of the Contract shall not be construed as a waiver of the violation or breach, or of any future violation or breach.

11.16 MEDIA RELEASES

- A. Contractor shall not use System Agency's name, logo, or other likeness in any press release, marketing material, or other announcement without System Agency's prior written approval. System Agency does not endorse any vendor, commodity, or service. Contractor is not authorized to make or participate in any media releases or public announcements pertaining to this Contract or the Services to which they relate without System Agency's prior written consent, and then only in accordance with explicit written instruction from System Agency.
- B. 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.

11.17 NO MARKETING ACTIVITIES

Contractor is prohibited from using the Work for any Contractor or third-party marketing, advertising, or promotional activities, without the prior written consent of System Agency. The foregoing prohibition includes, without limitation, the placement of banners, pop-up ads, or other advertisements promoting Contractor's or a third party's products, services, workshops, trainings, or other commercial offerings on any website portal or internet-based service or software application hosted or managed by Contractor as part of the Work.

11.18 PROHIBITION ON NON-COMPETE RESTRICTIONS

Contractor shall 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.

11.19 SOVEREIGN IMMUNITY

Nothing in the Contract shall be construed as a waiver of the System Agency's or the State's sovereign immunity. This Contract shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to the System Agency or the State of Texas. The failure to enforce, or any delay in the enforcement of, any privileges, rights, defenses, remedies, or immunities available to the System Agency or the State of Texas under the Contract or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. System Agency does not waive any privileges, rights, defenses, or immunities available to System Agency by entering into the Contract or by its conduct prior to or subsequent to entering into the Contract.

11.20 ENTIRE CONTRACT AND MODIFICATION

This 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.

11.21 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.

11.22 CIVIL RIGHTS

- A. Contractor shall comply with all applicable state and federal anti-discrimination laws, including:
 - i. Title VI of the Civil Rights Act of 1964 (42 U.S.C. §2000d, *et seq.*);
 - ii. Section 504 of the Rehabilitation Act of 1973 (29 U.S.C. §794);
 - iii. Americans with Disabilities Act of 1990 (42 U.S.C. §12101, *et seq.*);
 - iv. Age Discrimination Act of 1975 (42 U.S.C. §6101, *et seq.*);
 - v. Title IX of the Education Amendments of 1972 (20 U.S.C. §1681, *et seq.*);
 - vi. Food and Nutrition Act of 2008 (7 U.S.C. §2011, *et seq.*); and
 - vii. The System Agency's administrative rules, as set forth in the Texas Administrative Code, to the extent applicable to this Agreement.
- B. Contractor shall 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.
- C. Contractor shall 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 shall 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.

Contractor shall 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 shall comply with Section 504 of the Rehabilitation Act of 1973 and its implementing regulations at 28 CFR Subpart G § 42.503, and Americans with Disabilities Act of 1990 and its implementing regulations at 28 CFR Subpart B §35.130 which includes requiring contractor to make reasonable modifications in policies, practices, or procedures when the modifications are necessary to avoid discrimination on the basis of disability, unless the contractor can demonstrate that making the modifications would fundamentally alter the nature of the service, program, or activity.
- E. Contractor shall comply with federal regulations regarding equal treatment for faith-based organizations under 45 C.F.R. Part 87 or 7 C.F.R. Part 16, as applicable. Contractor shall not discriminate against clients or prospective clients on the basis of religion or religious belief, and shall provide written notice to beneficiaries of their rights.
- F. Upon request, Contractor shall provide the HHSC Civil Rights Office with copies of the Contractor's civil rights policies and procedures.
- G. Contractor must notify HHSC's Civil Rights Office of any civil rights complaints received relating to its performance under this Contract. 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
Fax: (512) 438-5885.

11.23 ENTERPRISE INFORMATION MANAGEMENT STANDARDS

Contractor shall conform to HHS standards for data management as described by the policies of the HHS Chief Data and Analytics Officer. 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 HHS for ongoing data governance, strategic portfolio analysis, interoperability planning, and valuation of HHS System data assets.

11.24 DISCLOSURE OF LITIGATION

- A. The Contractor must disclose in writing to the contract manager assigned to this Contract any material civil or criminal litigation or indictment either threatened or pending involving the Contractor. "Threatened litigation" as used herein shall include governmental investigations and civil investigative demands. "Litigation" as used herein shall include administrative enforcement actions brought by governmental agencies. The Contractor must also disclose any material litigation threatened or pending involving Subcontractors, consultants, and/or lobbyists. For purposes of this section, "material" refers, but is not limited, to any action or pending action that a reasonable person knowledgeable in the applicable industry would consider relevant to the Work under the Contract or any

development such a person would want to be aware of in order to stay fully apprised of the total mix of information relevant to the Work, together with any litigation threatened or pending that may result in a substantial change in the Contractor's financial condition.

- B. This is a continuing disclosure requirement; any litigation commencing after Contract Award must be disclosed in a written statement to the assigned contract manager within seven calendar days of its occurrence.

11.25 No THIRD-PARTY BENEFICIARIES

The Contract is made solely and specifically among and for the benefit of the Parties named herein and their respective successors and assigns, and no other person shall have any right, interest, or claims hereunder or be entitled to any benefits pursuant to or on account of the Contract as a third-party beneficiary or otherwise.

11.26 BINDING EFFECT

The Contract shall inure to the benefit of, be binding upon, and be enforceable against, each Party and their respective permitted successors, assigns, transferees, and delegates.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Exhibit G-1: HHSC Special Conditions



TEXAS

Health and Human Services

Health and Human Services Commission
Special Conditions
Version 1.2
9.1.17

|

Contents	
Article I. Special Definitions	1
Article II. General Provisions.....	1
2.01 Renegotiation and Reprocurement Rights.....	1
Article III. Contractors Personnel and Subcontractors	2
3.01 Qualifications	2
3.02 Conduct and Removal	2
Article IV. Performance	2
4.01 Measurement	2
Article V. Amendments and Modifications.....	3
5.01 Formal Procedure	3
5.02 Minor Administrative Changes	3
Article VI. Payment	3
6.01 Enhanced Payment Procedures	3
Article VII. Confidentiality	3
7.01 Consultant Disclosure	3
7.02 Confidential System Information	3
Article VIII. Disputes and Remedies.....	4
8.01 Agreement of the Parties	4
8.02 Operational Remedies	4
8.03 Equitable Remedies	5
8.04 Continuing Duty to Perform.....	5
Article IX. Damages.....	5
9.01 Availability and Assessment	5
9.02 Specific Items of Liability	6
Article X. Miscellaneous Provisions	6
10.01 Conflicts of Interest.....	6
10.02 Flow Down Provisions	7

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.

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

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

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

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

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

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

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

3.02 Conduct and Removal

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

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

Article IV. PERFORMANCE

4.01 Measurement

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

- (a) Compliance with Contract requirements, including all representations and warranties;
- (b) Compliance with the Work requested in the Solicitation and Work proposed by Contractor in its response to the Solicitation and approved by HHSC;
- (c) Delivery of Work in accordance with the service levels proposed by Contractor in the Solicitation Response as accepted by HHSC;
- (d) Results of audits, inspections, or quality checks performed by the HHSC or its designee;
- (e) Timeliness, completeness, and accuracy of Work; and
- (f) Achievement of specific performance measures and incentives as applicable.

Article V. AMENDMENTS AND MODIFICATIONS

5.01 Formal Procedure

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

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

5.02 Minor Administrative Changes

HHSC's designee, referred to as the Contract Manager, Project Sponsor, or other equivalent, in the Contract, is authorized to provide written approval of mutually agreed upon Minor Administrative Changes to the Work or the Contract that do not increase the fees or term. Changes that increase the fees or term must be accomplished through the formal amendment procedure, as set forth in Section 5.01 of these Special Conditions. Upon approval of a Minor Administrative Change, HHSC and Contractor will maintain written notice that the change has been accepted in their Contract files.

Article VI. PAYMENT

6.01 Enhanced Payment Procedures

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

Article VII. CONFIDENTIALITY

7.01 Consultant Disclosure

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

7.02 Confidential System Information

HHSC prohibits the unauthorized disclosure of 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 VIII. DISPUTES AND REMEDIES

8.01 Agreement of the Parties

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

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

8.02 Operational Remedies

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

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

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

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

8.03 Equitable Remedies

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

8.04 Continuing Duty to Perform

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

Article IX. DAMAGES

9.01 Availability and Assessment

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

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

9.02 Specific Items of Liability

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

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

IN COORDINATION WITH THE INDEMNITY PROVISIONS CONTAINED IN THE UTC, Contractor WILL BE SOLELY RESPONSIBLE FOR ALL COSTS INCURRED THAT ARE ASSOCIATED WITH INDEMNIFYING THE STATE OF TEXAS OR HHSC WITH RESPECT TO INTELLECTUAL, REAL AND PERSONAL PROPERTY. ADDITIONALLY, HHSC RESERVES THE RIGHT TO APPROVE COUNSEL SELECTED BY Contractor TO DEFEND HHSC OR THE STATE OF TEXAS AS REQUIRED UNDER THIS SECTION.

Article X. MISCELLANEOUS PROVISIONS

10.01 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.

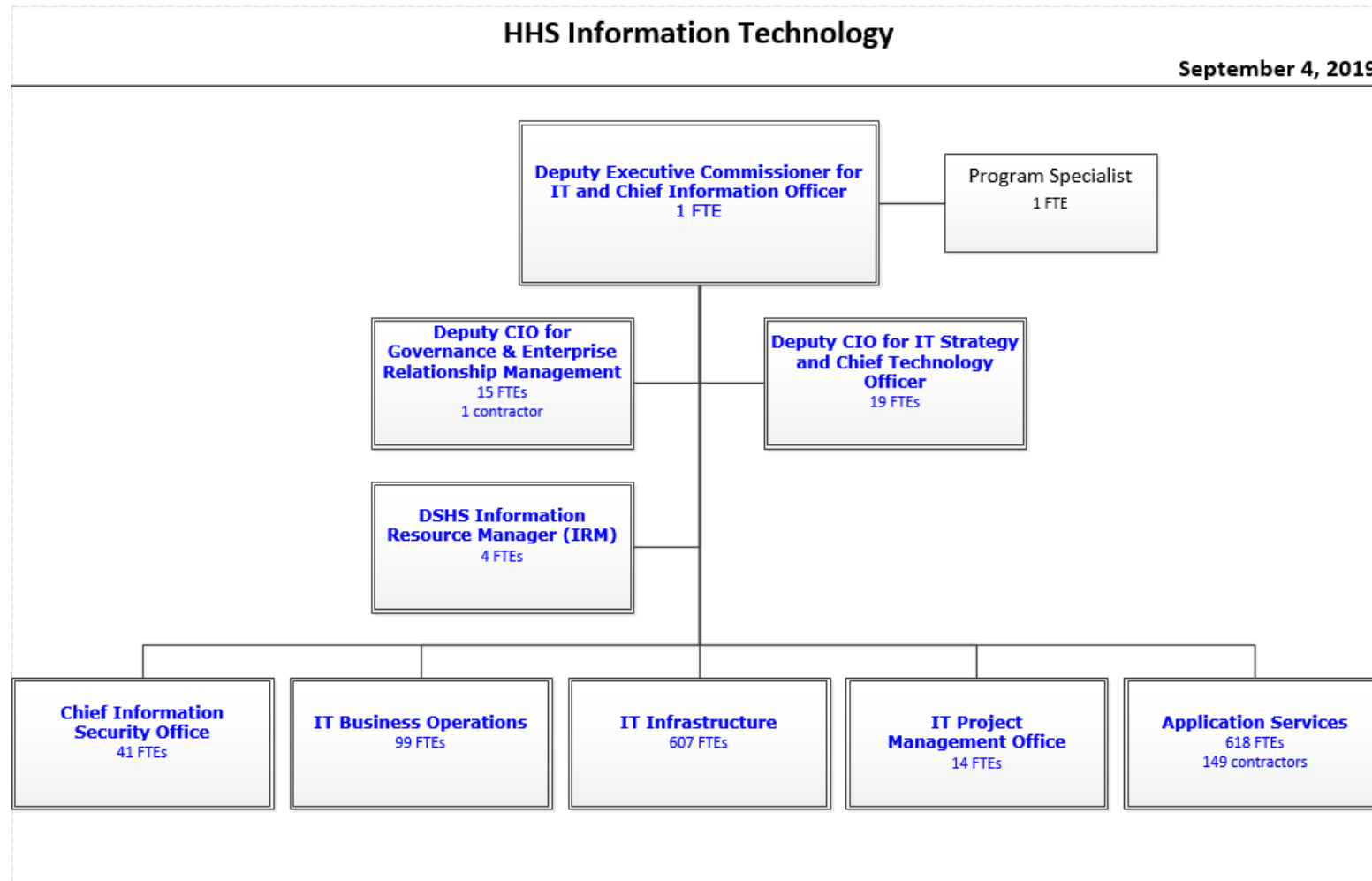
10.02 Flow Down Provisions

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 H: Scope of Work Supporting Documents

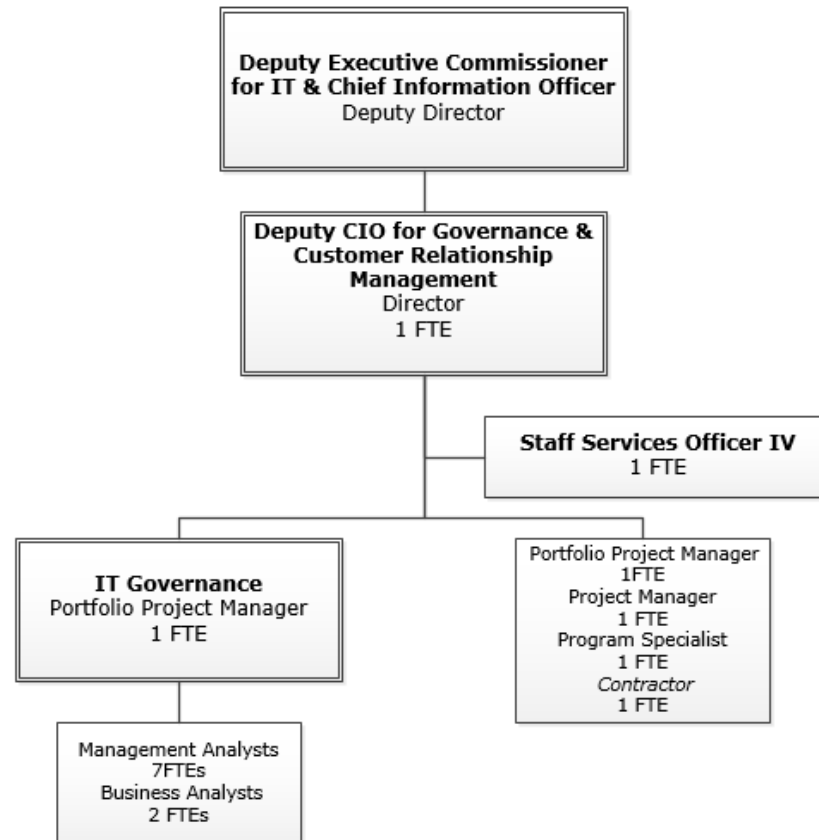
Exhibit H-1: HHSC IT Organizational Structure



HHS Information Technology

DCIO for Governance & Customer Relationship Management

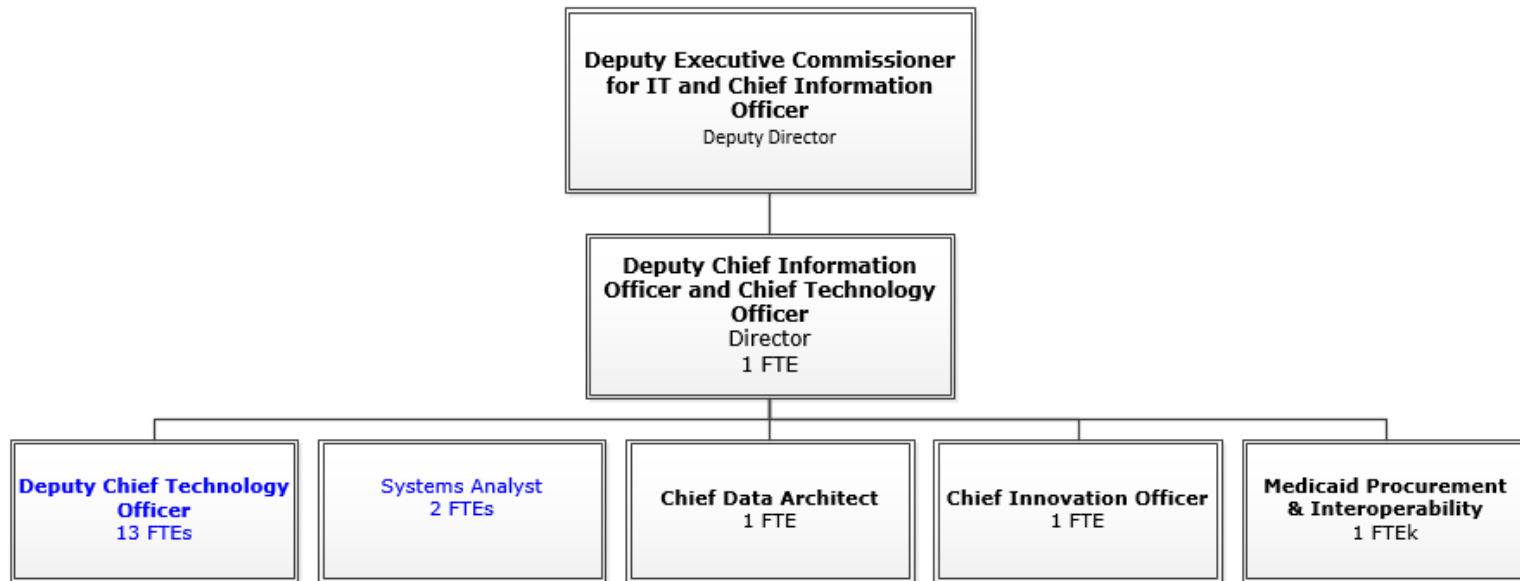
September 4, 2019



HHS Information Technology

Chief Technology Office (CTO)

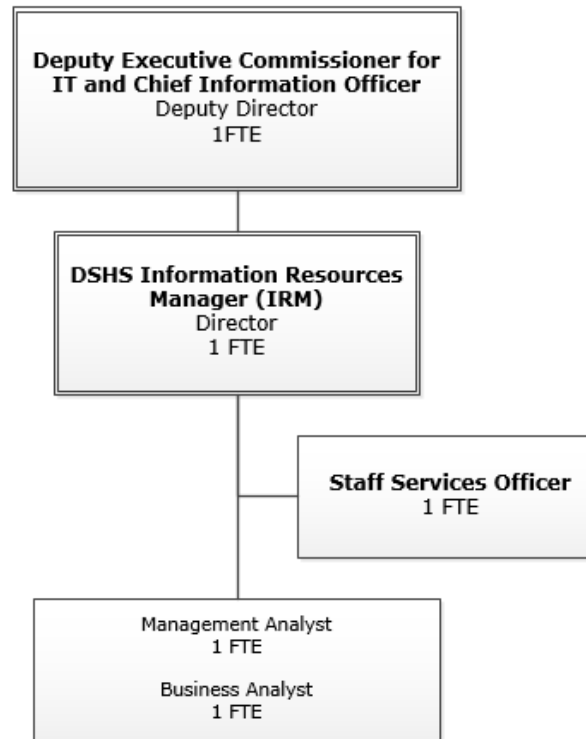
September 4, 2019



HHS Information Technology

DSHS Information Resource Manager

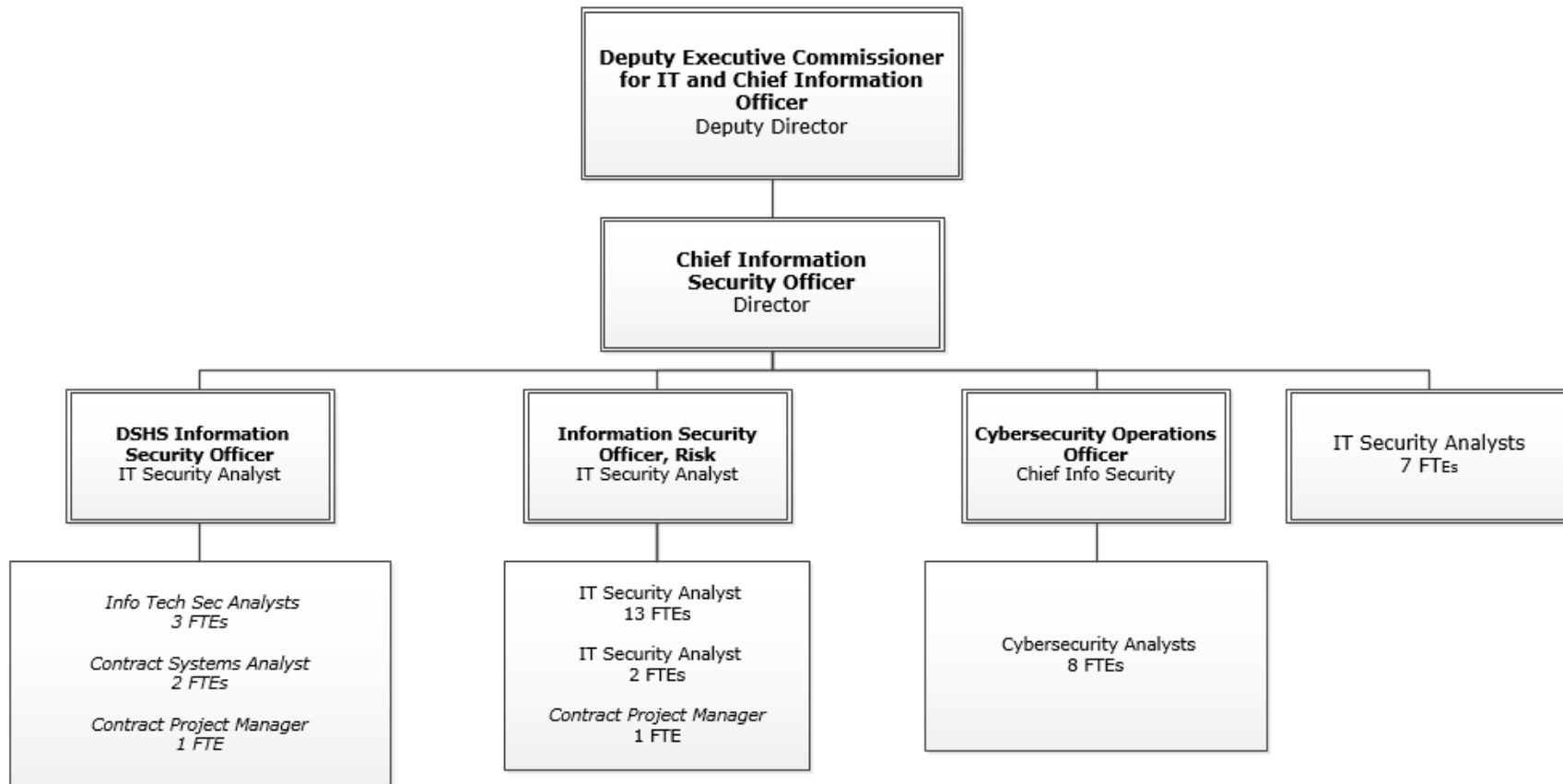
September 4, 2019



HHS Information Technology

CISO Chief Information Security Office

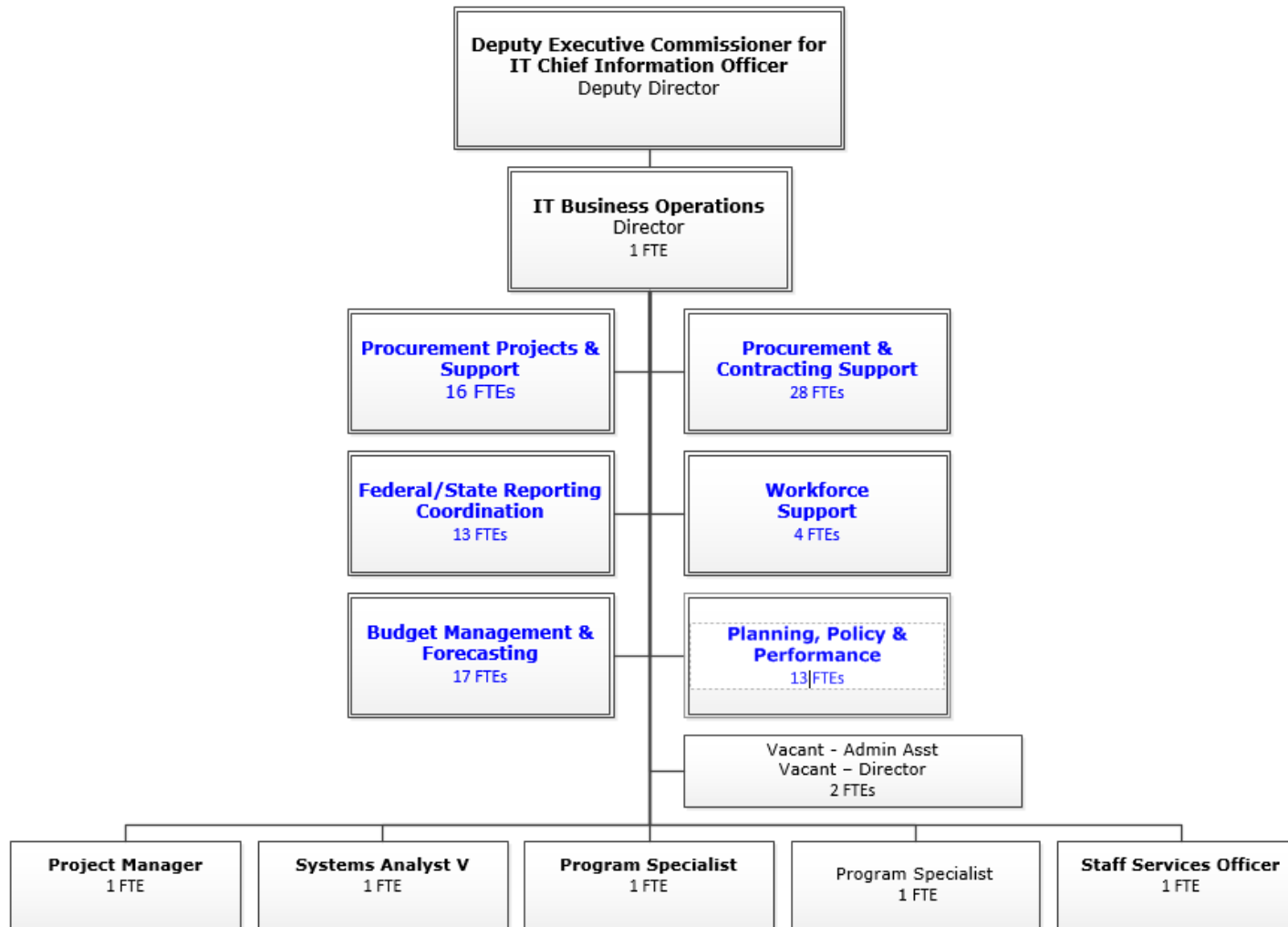
September 4, 2019



HHS Information Technology

IT Business Operations (ITBO)

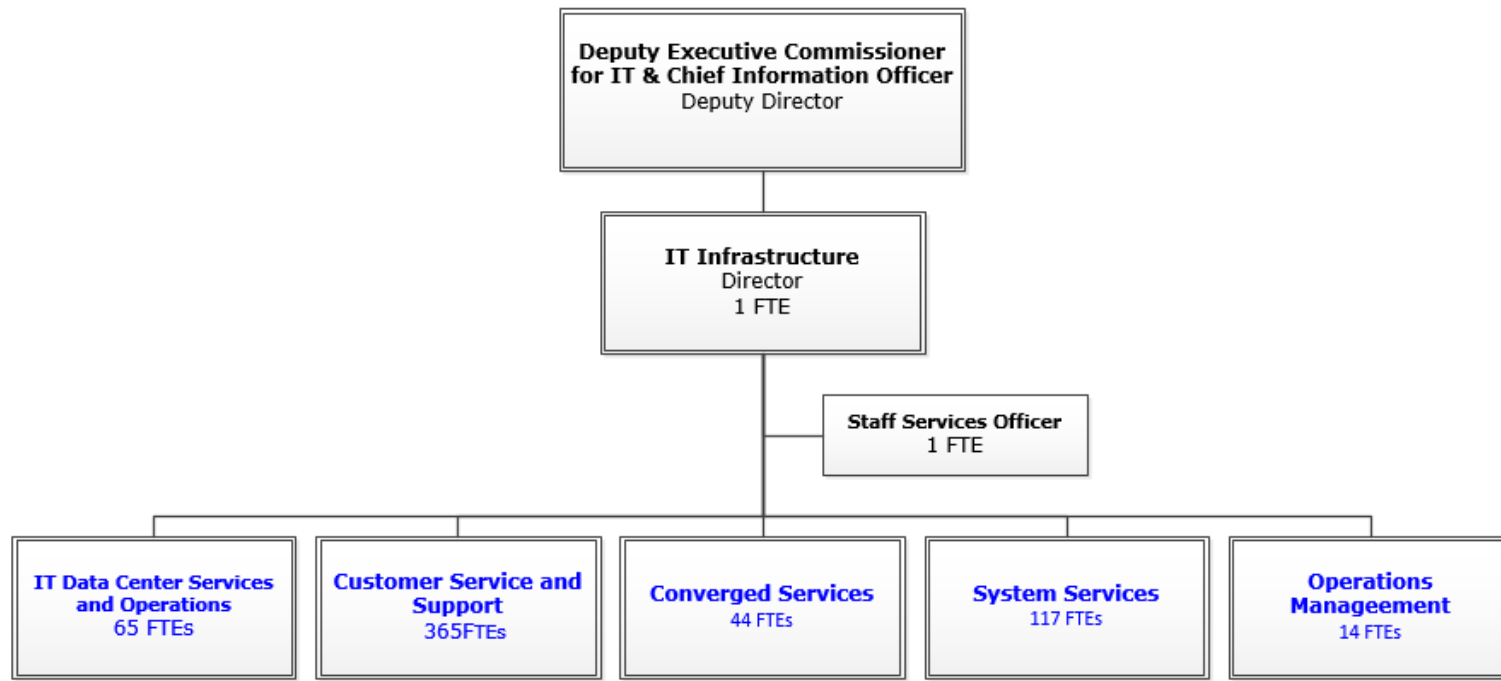
September 4, 2019



HHS Information Technology

IT Infrastructure

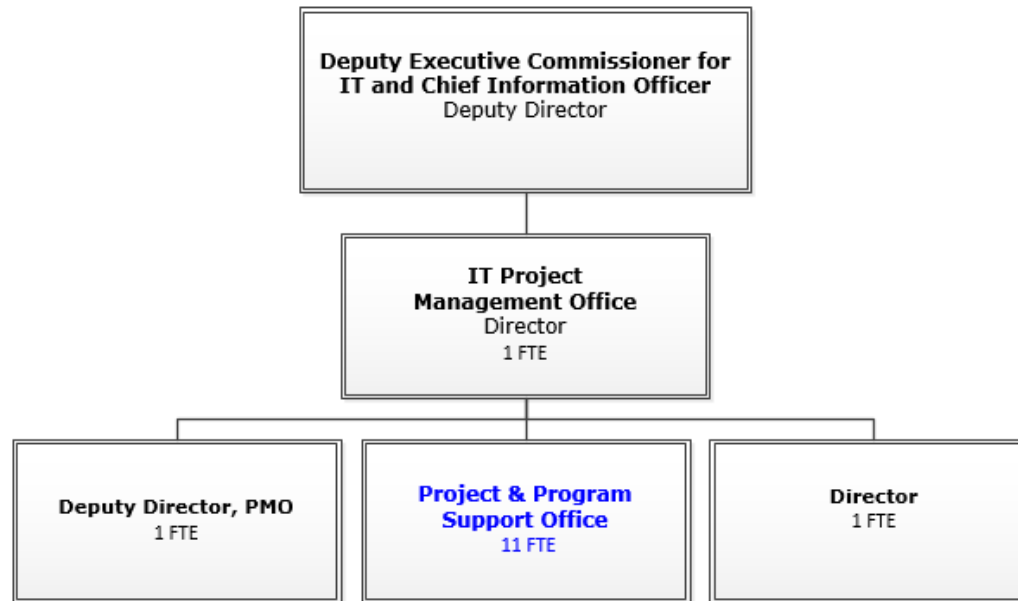
September 4, 2019



HHS Information Technology

IT Project Management Office (PMO)

September 4, 2019



HHS Information Technology

Application Services

September 2, 2019

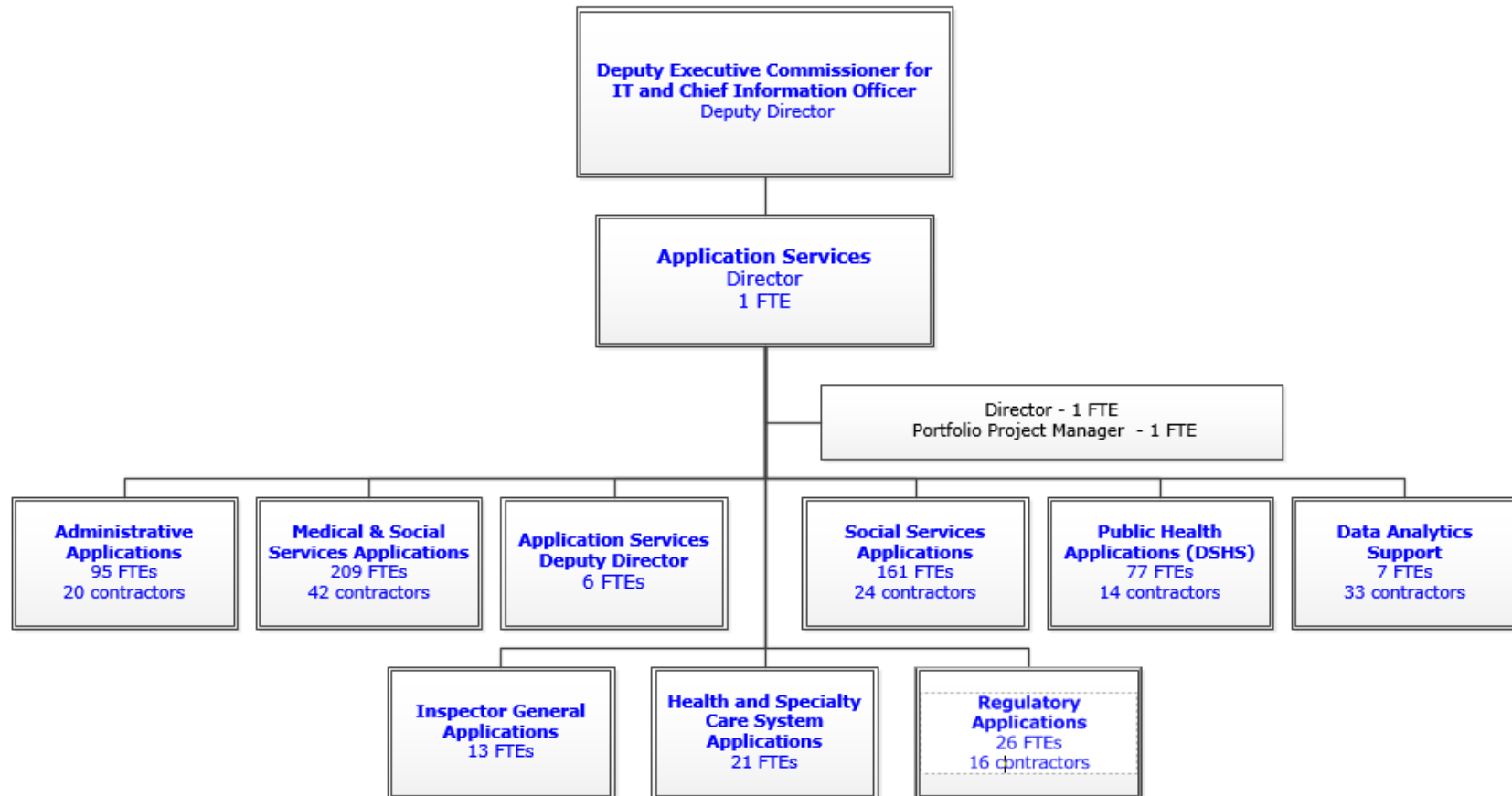


Exhibit H-2: Glossary

Term	Definition
AUA	Acceptable Use Agreement
AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
CFR	Code of Federal Regulations
CJIS	Criminal Justice Information Services
CIO	Chief Information Officer
CITO	Chief Information Technology Officer
CMS	Centers for Medicare and Medicaid Services
DBA	Data Base Administrator
DIR	Department of Information Resources
DSHS	Department of State Health Services
DUA	Data Use Agreement
EIS	Enterprise Information Security
EPLS	Excluded Parties List System
ESSI	Enterprise Single Sign-on
FERPA	Family Educational Rights and Privacy Act
FFATA	Federal Funding Accountability and Transparency Act
FICA	Federal Insurance Contributions Act
FIPS	Federal Information Processing Standard
FIN	Finance
FLSA	Fair Labor Standards Act
FNS	Food and Nutrition Service
FTE	Full time equivalent
FTI	Federal Tax Information
GAAP	Generally Accepted Accounting Principles
GASB	Governmental Accounting Standards Board
HHS	Health & Human Services
HHSC	Health & Human Services Commission
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
HSP	HUB subcontracting plan
HUB	Historically under-utilized business
ID	Identification
IM	Instant Messaging
IP	Internet Protocol
IR	Information Resources
IRM	Information Resource Manager
IRS	Internal Revenue Service
IS	Information Security
ISP	Internet Service Provider

Term	Definition
IT	Information Technology
ITBO	Information Technology Business Operations
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
P2P	Peer-to-peer
PDF	Portable Document Format
PIA	Public Information Act, Chapter 552 of the Texas Government Code
PII	Personal Identifying Information
PHI	Personal Health Information
PL	Public Law
Q&A	Question and Answer
SAM	System for Award Notification
SAO	State Auditor's Office
SFTP	Secure File Transfer Protocol
SPI	Security and Privacy Inquiry
SOW	Statement of Work
SSA	Social Security Administration
SSA	Support Services Agreement
SSN	Social Security Number
TAC	Texas Administrative Code
TEC	Texas Ethics Commission
TGC	Texas Government Code
TGL	Technical Guidance Letter
TIERS	Texas Integrated Eligibility Redesign System
TVPA	Trafficking Victims Protection Act
UPS	United Parcel Service
USB	Universal Serial Bus – industry standard for cables, connectors and protocols
USC	United States Code
UTCs	Uniform Terms and Conditions
VPN	Virtual Private Network
WIFI	Wireless local area network

Exhibit H-3: DRAFT Support Services Agreement

DRAFT ---- Support Services Agreement ---- DRAFT HHSC Information Technology Baseline Services

SECTION 1 – Preamble

In compliance with Texas Government Code Sections 531.02012 and 531.00553, this support services agreement (SSA) operationalizes Circular C-051 and outlines at a high level the centralized services that the Health and Human Services Commission (HHSC) will receive from HHSC Information Technology. This SSA also includes performance goals that Information Technology must meet and defines the fundamental roles and responsibilities of the respective areas related to Information Technology services.
In compliance with Texas Government Code Section 531.0055(k)(4), Executive Commissioner: General Responsibility for Health and Human Services System, this SSA ensures HHS agencies share data and information needed to carry out their respective functions, unless otherwise prohibited by law.

SECTION 2 – Overview

A. Overview of HHSC Information Technology

Mission

The HHSC Information Technology (IT) division's mission is to provide outstanding customer service and innovative technology solutions securely, efficiently, and effectively.

Organizational Structure

HHSC IT has created a new IT organizational structure to support the HHS system. As shown in the table below, the new organization includes the following nine departments.

- Deputy Chief Information Officer for IT Strategy
- Deputy Chief Information Officer for Governance and Enterprise Relationship Management
- DSHS Information Resource Manager
- Chief Information Security Officer
- Director of Business Operations
- Director of IT Infrastructure
- Director of Application Services
- Director of the Project Management Office

IT Governance

HHSC IT coordinates a governance structure with representation from all major customers at appropriate organizational levels to participate in IT decision making. A primary goal of governance is to provide a decision framework and processes to make investment decisions and drive business value. Governance looks to incorporate business, technology, and data to ensure that HHSC IT is aligned with program strategy.

The IT Governance model includes 6 business portfolios and 2 system-wide portfolios:

- Public Health Services
- Administrative
- Medical and Social Services
- Regulatory Services
- Health and Specialty Care System
- Inspector General
- Infrastructure and Shared Services (system-wide)
- Portal Authority (system-wide)

IT has an intake process to help address Program's business needs. During this intake process IT will partner with Program to:

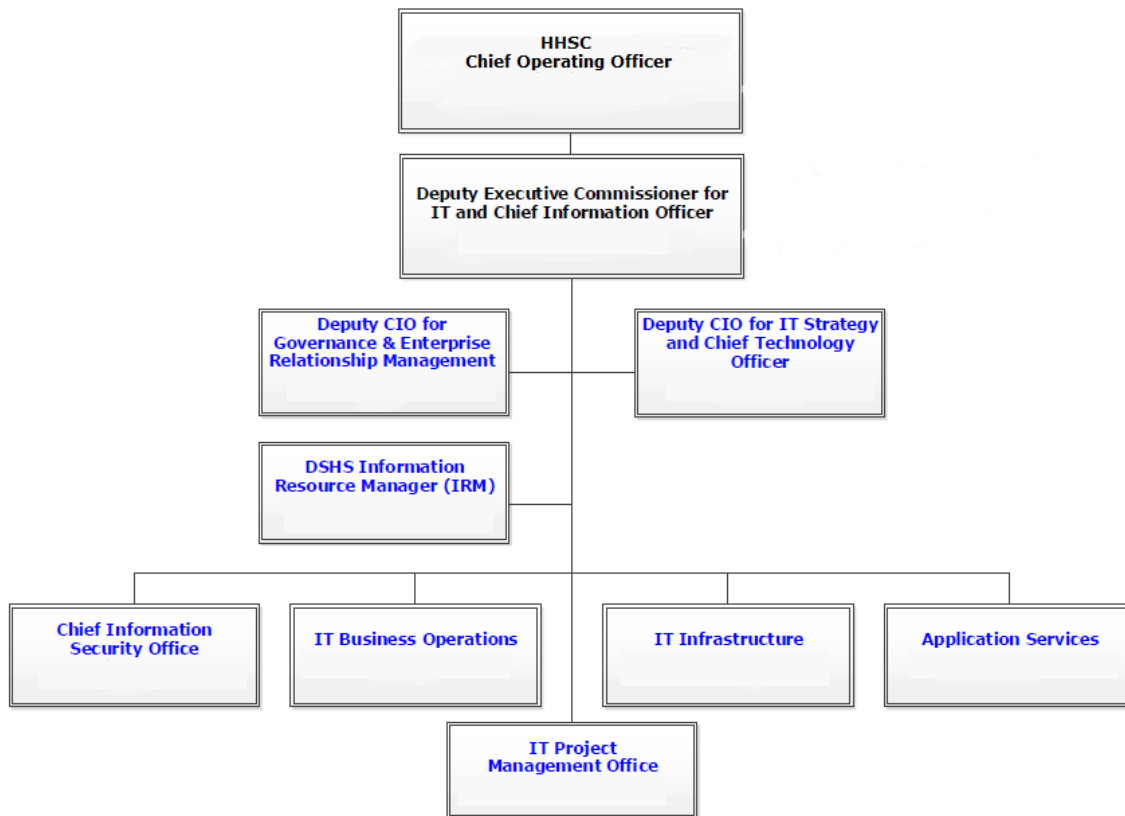
- understand the business need,
- propose solutions,
- confirm that proposed solutions meet the business need, and
- ensure that Program can prioritize the efforts based on resources and capacity.

The guiding principles for the Intake Process are:

- Align with program strategy and priority.
- Focus on business outcomes and manage risk.
- Keep IT resources focused on added value activities that are aligned with initiatives that have been approved through the governance process.
- Consider full lifecycle costs (project and on-going).

B. Organization Chart for the Information Technology (FY19)

July 2, 2019



SECTION 3 – Requestable Services

This section includes services that can be requested by program and support service areas.

A. Applications

A.1. SharePoint

Service Provider:	Applications
Description:	Assists those requesting new SharePoint sites. Creates SharePoint sites for agency users and sets users up with basic SharePoint functionality.

A.2. TxEVER (Texas Electronic Vital Events Registrar) Help Desk

Service Provider:	Applications
Description:	Provides TxEVER application help desk support. The TxEVER system supports all vital events operations, including reporting, registration, and amendments of births and deaths.

A.3. TIERS Help Desk

Service Provider:	Applications
Description:	Provides analytical, system, and program assistance to all TIERS users. Handles issues (including but not limited to process issues, policy, data entry, defects or modifications) relating to TIERS, Self-Service Portal, State Portal, TLM, Scheduler, TIERS Mobile applications, as well as other agency and non-agency software interfaces.

A.4. Salesforce—Application Development

Service Provider:	Applications
Description:	New application development. Provides customized Salesforce solutions to meet the needs of the agency. Provides tools to help manage customer relationships, including gathering and organizing customer information

(for example, financial information) to produce reports and analytics.

A.5. Application Modification

Service Provider:	Applications
Description:	Oversees and makes minor changes or modifications to existing applications. This may require review by a Change Management Board.

A.6. New IT Application

Service Provider:	Applications Development
Description:	This service is part of the larger IT Project Request Process. This service is initiated when a customer needs to find a solution to a stated program need. Solution may include developing or purchasing an application or tool or creating a process. As part of this service, this area will work with agency programs to assess the priority and criticality of their needs in order to customize deliverables to the program's specific needs and requirements.

A.7. Medicaid Management Information System (MMIS) Enhanced Funding

Service Provider:	Applications
Description:	Provides assistance with Advance Planning documents (APD) in order to qualify for MMIS funding. This service offers resources to draft the APD to include CMS (Centers for Medicare and Medicaid) standard language, budget tables, and other required attachments.

A.8. Request for Proposal (RFP) Creation for IT Applications

Service Provider:	Applications
Description:	When a customer needs an IT solution for a specific business need, this service provides support that may include coordinating and facilitating the creation and completion of RFPs for IT applications.

A.9. Contract Consulting for IT Applications

Service Provider:	Applications
Description:	Provides as-needed consultation reviews for existing and new contracts to ensure that contracts are compliant with all IT components. Part of a process of ongoing review and oversight by HHS IT.

B. Business Operations

B.1. Procurement Approach Consulting

Service Provider:	IT Business Operations Major Procurements
Description:	This service assesses the customer's business need in order to determine the appropriate procurement approach or process. This service assists the customer to establish a high-level scope and timeline for the procurement, along with a strategy for executing the optimal contract approach within the shortest timeline.

B.2. Procurement Project Management

Service Provider:	IT Business Operations Major Procurements
Description:	This service provides task-level management and monitoring of the procurement schedule. Project Management services may be obtained for the end-to-end procurement lifecycle, or limited to one or more components, e.g., grant preparation and submission (CMS/FNS), business analysis, procurement and evaluation, and final external approvals and execution.

B.3. Procurement Business Analysis

Service Provider:	ITBO Major Procurements
Description:	Business Analysis includes facilitation of meetings with stakeholders and executives to identify, refine, and validate business and technical requirements.

B.4. Statement of Work/Request for Offers/Request for Proposals Drafting

Service Provider:	ITBO Major Procurements
Description:	This service offers resources to draft the RFP/RFO to include PCS standard language, formatted requirements, terms and conditions, and other required attachments. Includes compilation of a procurement library, if necessary. Includes development of the evaluation tool.

B.5. Federal and State Reporting and Coordination

Service Provider:	IT Business Operations
Description:	<p>Work with appropriate stakeholders (program management, IT management, project managers) to develop high quality content for major information resources project documentation to ensure appropriate review cycles for approval, and submission to the appropriate entities to ensure project approval, federal financial funding participation, and project compliance with all state and federal regulations.</p> <p>The Federal State Coordination team also works with program and IT management regarding strategy for active and proposed major information resources projects, and provides expert consultation regarding federal and state regulations, processes, procedures and best practices for submission.</p>

C. Chief Technology Office

C.1. Business Architecture Engagement

Service Provider:	Chief Technology Office
Description:	Collaborate with program area stakeholders to understand priority initiatives and translate business strategy into defined technological needs, strategy statements, and action steps that establish a path to the desired future state implementation.

C.2. Architecture Consultation

Service Provider:	Chief Technology Office
Description:	Provides detailed guidance on infrastructure technologies, reference architecture, best practices, methodologies and case studies on technology strategies and solutions.

C.3. Applications Architecture Strategy

Service Provider:	Chief Technology Office
Description:	Provides strategies and roadmaps for enterprise applications architecture across the agency with the following goals: to establish and document enterprise-wide standards, best practices and reusable software components; and to ensure that the technical solutions are consistent with the long-term HHSC IT strategy and approved technology standards.

C.4. Enterprise System Architecture

Service Provider:	Chief Technology Office
Description:	Provides strategy and roadmaps for infrastructure architecture across the agency that promote solutions based on current, emerging technologies, that are cost effective, and that meet functional, technical, and performance requirements. Provides technical leadership on project engagements, serves as a technical resource, and develops proposals for, with analysis of, alternative solutions.

D. IT Chief Information Security Office (CISO)

D.1. System Categorization, Project Support, and Procurement Support

Service Provider:	Chief Information Security Office
Description:	HHS Information Security assists with determining the relevant security requirements for HHS information systems, projects, and procurements.

D.2. System Security Plans and Information System Risk Assessments

Service Provider:	Chief Information Security Office
Description:	HHS Information Security assists program areas with the developing information system security plans and conducting annual information system risk assessments.

D.3. Vulnerability Assessments and Penetration Testing

Service Provider:	Chief Information Security Office—HHS Cybersecurity Operations Center
Description:	HHS Cybersecurity Operations Center provides network, system, and application vulnerability assessments and penetration testing for HHS information systems.

D.4. Independent Security Assessments

Service Provider:	Chief Information Security Office
Description:	HHS Information Security conducts independent security assessments of HHS information systems.

D.5. Contract Oversight and Monitoring Advice

Service Provider:	Chief Information Security Office
Description:	HHS Information Security advises program areas on the security impact that contractor-reported non-compliance poses to HHS data.

D.6. Audit Support

Service Provider:	Chief Information Security Office
Description:	HHS Information Security provides advice concerning internal, Texas, and federal audit responses that contain information security requirements.

D.7. Information Security Awareness Program

Service Provider:	Chief Information Security Office
Description:	HHS Information Security maintains and supports the overall HHS information security awareness program. Annual mandatory computer-based security awareness training is provided through HHS System Training Solutions.

D.8. Incident Response

Service Provider:	Chief Information Security Office
Description:	HHS Cybersecurity Operations Center provides assistance with security concerns, issues, and incidents.

E. Converged Services

E.1. Virtual Private Network (VPN)

Service Provider:	Converged Services
Description:	Provides remote Virtual Private Network (VPN) access to HHS enterprise Network. This includes employee and vendor remote access as well as point-to-point VPN Tunnel access.

E.2. Contact Center Services

Service Provider:	Converged Services
Description:	<p>Services for basic and advanced call center support that include automatic call distribution, integrated voice response, teleworking, call back assist (virtual hold), virtual/desktop wall board, workforce, quality management, call recording (audio and video), and reporting/analytics.</p> <p>*Note: New or major support might require going through the IT Governance Process.</p>

E.3. Basic and Advanced Phone Service

Service Provider:	Converged Services
Description:	Services for basic and advanced phones such as Toll-Free (1-800) numbers, dialtone as a service, attendant soft phones, voicemail services, and long distance / international dialing.

E.4. Teleconferencing—Public Hearing Teleconferencing (PHTC)

Service Provider:	Converged Services
Description:	A system capability that enables a service that has a moderator and allows a presenter to talk to many listeners. The moderator controls the speaker and controls the question and answer sessions.

F. Customer Service and Support

F.1. Health and Specialty Care Systems Customer Support

Service Provider:	Customer Service and Support
Description:	<p>Health & Specialty Care System (HSCS) Customer Support provides statewide workstation, network, and end user support services to the following:</p> <ul style="list-style-type: none">• State Supported Living Center (SSLC) Support• State Hospital Support <p>Standard support is provided from 8 a.m. to 5 p.m. Monday through Friday with on-call support after hours and on state holidays.</p>

F.2. IT Customer Service Help Desk

Service Provider:	Customer Service and Support
Description:	<p>The HHSC IT Customer Service (ITCS) Help Desk is the central point of contact for requesting IT Support. The HHSC ITCS Help Desk consists of:</p> <ul style="list-style-type: none">• Consolidated/Enterprise Help Desk• TIERS/IEE Help Desk• DFPS Help Desk• CARE Application Support• Legacy DARS Support

F.3. Regional and State Office Customer Support

Service Provider:	Customer Service and Support
Description:	<p>Regional and State Office Customer Support is an organization that provides IT support operations throughout the state.</p> <ul style="list-style-type: none">• HHSC Deskside Support• DSHS Deskside Support• WIC Office Support

G. Data Center Services

G.1. DCS Delivery

Service Provider:	Data Center Services
Description:	<p>Data Center Service Delivery provides oversight for infrastructure and operational services to the non-TIERS user-community, twenty-four hours a day, seven days a week and 365 days a year.</p> <p>Data Center Service Delivery supports computing resources to meet the business requirements, including the analysis of servers, migration of data, new infrastructure/environments, on-going support, issue resolution, and product updates.</p> <p>Data Center Service Delivery provides focused, cost-optimized, consistent managed data center services are provided to HHS programs.</p> <p>Infrastructure/Computing services offered include: Application, Storage, Cloud, Compute, Database, DIR MAS and MSS, Texas.Gov, File Services, Middleware, Monitoring, Print/Mail Services, Reporting, Web Hosting, SFTP (via Globalscape, TX FTI Hub)</p>

G.2. DCS Disaster Recovery Services

Service Provider:	Data Center Services
Description:	HHS IT Disaster Recovery is the HHS point of contact for questions regarding Application Disaster Recovery process, procedures, and testing, and represents HHS in

- | |
|--|
| IT disaster recovery related audits. Disaster Recovery Services include: |
| <ul style="list-style-type: none"> • Evaluation of IT disaster recovery strategies and procedures • Development and implementation of IT Disaster Recovery plans • Coordination of disaster recovery plans, exercises, documentation, and services • Review and evaluation of risk assessment, business impact analysis, disaster recovery test planning proposals, and materials for HHS critical mission applications and/or business programs |

G.3. DCS-Enterprise Secure FTP Support (SFTP)

Service Provider:	Data Center Services
Description:	This service streamlines the exchange of confidential data for HHSC and its affiliates. HHSC users are able to exchange data on highly reliable secure connections which meet technical guidelines for safe and secure data transactions.

G.4. DSHS and HHSC DCS-Resource Management

Service Provider:	Data Center Services
Description:	This service provides DCS customers incident, change, and problem management support; are agency approvers for changes in the weekly Change Advisory Board meetings. Submits and approves customer requests for services. Approves security and DCS tool access requests. Coordinates project document approvals, including financial approval. Works with service providers to resolve customer issues as a first level escalation.

G.5. DCS-Enterprise Reporting Mental and Behavioral Health Outpatient Warehouse (MBOW) Data Warehouse Support

Service Provider:	Data Center Services
Description:	The Enterprise Reporting Environment unit oversees reporting environments shared by HHSC, DSHS, and health providers. Provides specialized business intelligence analytical reporting to assist with business resolution by compiling metadata, to produce real-time tracking trends, data discovery, patterns and insights. The data warehouse, MBOW (Mental and Behavioral health Outpatient Warehouse), collects Local Mental Health Authority (LMHA) encounter data from State Community Centers, integrates with CARE data (via an operational data store), Medicaid eligibility data and authorization data to produce analyses for HHSC and its affiliates.

H. IT Governance

H.1. IT Governance Office

Service Provider:	IT Governance
Description:	The objective of IT governance is to ensure the effective and efficient use of IT in enabling an organization to achieve its goals. HHSC IT facilitates and supports IT governance, a decision framework and process that allows program executives to make data-based IT investment decisions that drive business value. IT governance clarifies the decision rights and accountability for both program and IT leadership roles. The governance framework will apply to key decisions regarding IT strategy, technical roadmaps, and project prioritization. See Attachment C for a more detailed description of the Governance process.

I. System Services

I.1. Network Provisioning Services

Service Provider:	System Services
Description:	Access provisioning/deprovisioning of HHS network resources, including shared folders, calendars and mailboxes, distribution lists, network account

management, and VPN with and without two-factor authentication.

I.2. Password Manager Enterprise Single Sign-on (ESSO)

Service Provider:	System Services
Description:	Secure storage of credentials for individual users of HHS information resources and automatic login to HHS information resources based on successful Windows authentication.

I.3. Access Management

Service Provider:	System Services
Description:	Request access to 75+ HHS information resources. Automated approval workflows. Central Single SignOn enabled authentication port to 50+ HHS information resources. Automated provisioning and deprovisioning services for dozens of HHS information resources.

I.4. Application Provisioning Services

Service Provider:	System Services
Description:	Access provisioning and deprovisioning of 50+ application-based HHS information resources.

I.5. Video Conference Service

Service Provider:	System Services
Description:	Provides video conference services to HHS.

I.6. Hardware Asset Management

Service Provider:	System Services
Description:	Seat Management provides end user computing devices (tablets, laptops, and desktops) through a Hardware Acquisition and Leasing contract. Services are provided under a separate contract which includes; deployments services (de-install/install), on-site break fix support and return services. Equipment is refreshed every 3 to 4

years. Manages hardware assets through the product lifecycle. Manages hardware leasing of personal computers and seat management services contracts.

I.7. Automation and Image Management

Service Provider:	System Services
Description:	Provides HHS base image that consists of standard configuration for computers. Service Center Console Management (SCCM) administration. Configures and deploys approved software packages.

I.8. Software Asset Management (SAM)

Service Provider:	System Services
Description:	SAM provides oversight of policies and governance of matters pertaining to software licensing, tracking, compliance, authorization/approval of software, financial aspects of software needs, usage, forecasting, and potential liabilities.

I.9. Local Office Infrastructure (LOI)

Service Provider:	System Services
Description:	Supports the local office servers, Data Center Services (DCS) storage access, and performs backups on non DCS servers and subsets of personal computers.

I.10. New Cellular Services Accounts

Service Provider:	System Services
Description:	New Cellular Services Accounts

I.11. Cellular Services

Service Provider:	System Services
Description:	Provisions, maintains and de-provisions system-wide cellular services for all approved mobile carriers.

I.12. Teleconferencing—Audio/Video Teleconferencing

Service Provider:	System Services
Description:	A service that allows multiple users to connect and have a conversation and share video. The service can be reserved, or reservation-less and may have one or more leads/participants.

I.13. Related Services - Language Support

Service Provider:	System Services
Description:	A HHS supported and paid for service to support languages other than English and Spanish.

I.14. Incident Management Processes/Communication/Restoration/Remedial Action

Service Provider:	System Services
Description:	Ensures all operational entities within HHS follow the Incident Management Process. Updates agency leadership of restoration progress through regular communications. Coordinates the restoration of IT service outages to normal service operation levels as quickly as possible. Documents remediation actions.

I.15. E-Discovery Services

Service Provider:	System Services
Description:	IT Litigation support for HHS Legal and collaborative efforts across HHS. HHS eDiscovery develops, administers, and supports the process and technology through which electronically stored information (ESI) is searched, collected, preserved, analyzed, reviewed and produced for legal, investigative and regulatory proceedings as well as fulfill open record request.

SECTION 4 – HHS Support Services

This section includes services that are routinely provided to all program and support service areas as ongoing services without program or support service area request.

1. Continuous Monitoring

Service Provider:	Chief Information Security Office
Description:	<p>HHS Information Security and Cybersecurity Operations Center support the continuous monitoring of HHS information systems to ensure ongoing compliance with HHS security uniform.</p> <p>HHS Information Security provides this service for all registered information systems that reside in the organization's system catalog, are hosted in an HHS or State of Texas data center, and have an accurate asset inventory in their System Security Plan.</p>

2. Information and Data Architecture

Service Provider:	Chief Technology Office
Description:	<p>Provide an agency-wide technology governance roadmap to promote the overall availability, usability, integrity and security of the data. This consists of a governing body or council, a defined set of procedures and a plan to execute those procedures. Establish data analytics and virtualization platforms that can combine data from multiple sources or systems.</p>

3. New and Emerging Technology, Proof of Concepts, Application Pilots and Reference Implementations

Service Provider:	Chief Technology Office
Description:	Research new technologies to identify those with potential to improve technological capability or efficiency in future IT projects. Conduct proof-of-concept studies and pilot testing for new technologies that may be applied to business needs based on emerging disruptive technologies such as cloud computing, mobile technologies, social media, and big data. Partner with private sector research firms and vendors to inform agency regarding the current IT state-of-the-art and conduct of POCs.

4. Local Area Network (LAN)

Service Provider:	Converged Services
Description:	Install and test network hardware and software. Initiate tuning and capacity planning activities to enhance network performance. Evaluate network hardware and software to identify strengths, weaknesses, and potential benefits to the agency. Operational 24/7 Support. Maintain the operating system and security software utilized on network.

5. Wide Area Network (WAN)

Service Provider:	Converged Services
Description:	Install and test wireless network hardware and software. Initiate tuning and capacity planning activities to enhance wireless network performance. Evaluate wireless network hardware and software to identify strengths, weaknesses, and potential benefits to the agency. Maintain the operating system and security software utilized on agency wireless network.

6. Wireless Local Area Network (WLAN)

Service Provider:	Converged Services
Description:	Install and test wireless network hardware and software. Initiate tuning and capacity planning activities to enhance wireless network performance. Evaluate wireless network hardware and software to identify strengths, weaknesses, and potential benefits to the agency. Maintain the operating system and security software utilized on agency wireless network.

7. Perimeter (Access and Security)

Service Provider:	Converged Services
Description:	Install and test perimeter network hardware and software. Initiate tuning and capacity planning activities to enhance perimeter network performance. Evaluate perimeter network hardware and software to identify strengths, weaknesses, and potential benefits to the agency. Maintain the operating system and security software utilized on agency perimeter network. Provide support for Perimeter Distribution and Routers, Firewalls, Email Security Appliances (ESA), Web Security Appliances (WSA), F5 Load Balancers, Intrusion Protection System (IPS), IXIA and Fireeye (Joint with SecOps).

8. Customer Care

Service Provider:	Customer Service and Support
Description:	Customer Care staff are responsible for <ul style="list-style-type: none">• Escalations of complex and high business impact tickets• IT Alerts• IT Move Coordination• Project Management

9. DCS TIERS Operations

Service Provider:	Data Center Services
Description:	TIERS Operations delivers infrastructure and operational services to the TIERS user community on a twenty-four hours a day, seven days a week and 365 days a year basis.

10. IT DCS-Winters Data Center

Service Provider:	Data Center Services
Description:	This service provides physical hosting services in the Winters Data Centers. Among the services provided are 24/7 physical security and access control, conditioned power with UPS and generator backup, environmental monitoring, humidity and temperature control, fire suppression, and network connectivity.

11. IT Staff Augmentation Support

Service Provider:	IT Business Operations
Description:	Facilitates IT staffing requests, onboarding, termination, invoicing and reporting for all staff augmentation contractors obtained via the Department of Information Resources Information Technology Staff Augmentation contracts.

12. IT Contract Support

Service Provider:	IT Business Operations
Description:	Serves IT contract managers who need to acquire goods and services for their business needs. Assists customers who need to generate Statements of Work and Business Plans. Ensures that the customer has an actionable package of documents and a comprehensive strategy for completing the procurement.

13. Directory Services

Service Provider:	System Services
Description:	<p>This service creates network accounts that provide access management to agency resources. Services include:</p> <ul style="list-style-type: none">• Active Directory management for 25 domains across• Maintenance of Domain Name System (DNS) settings. Federated active directory services <p>Active directory integrated Dynamic Host Configuration Protocol (DHCP) services.</p>

14. Email/Security

Service Provider:	System Services
Description:	<p>This service ensures the secure delivery of Microsoft Office 365 email services.</p>

15. Office 365 (O365) Services/Collaboration Tools/Authentication

Service Provider:	System Services
Description:	<p>Provides daily delivery of Microsoft O365 application services including Skype, Teams, group calendars, mailboxes - as well as conference rooms, distribution lists, and service accounts. Provides daily delivery of Microsoft O365 AzureAD Multifactor Authentication (MFA).</p>

SECTION 5 – Roles and Responsibilities

The partnership between HHSC IT and its customers requires full, proactive participation from both parties. Some policies and procedures that are in place outlining this participation include:

- When providing direction or guidance to HHS agencies or programs on issues, policies, or procedures that may involve more than one administrative support area, support areas should strive to provide timely, coordinated guidance to HHS management and staff. As appropriate, direction or guidance should be consistent across the administrative support areas in an effort to support HHS

agencies and programs in effective decision making and administration of programs and functions.

- HHS Circular C-009 establishes centralized information systems planning authority including the authority of HHS IT to develop system-wide policies and procedures for the management of information technology functions.
- HHS Circular C-021 establishes the authority, role, and responsibility of HHS Information Security/Cybersecurity for maintaining an information security program, overseeing the information security functions of the HHS system, and establishing authority at the agency levels for implementing the Information Security (IS) objectives.
- HHS Circular C-050 requires the Deputy Executive Commissioner for IT to submit an operational plan discussing goals and major initiatives for the upcoming fiscal year. The plan will identify strategies and clearly defined activities to achieve goals and successfully implement major initiatives.
- System-wide Information Technology policies, standards, processes, and procedures are defined and located on a SharePoint site.
- Procurement and Contracting Services' Handbook of Operating Procedures, in policy OP 700, requires HHS agencies to receive prior approval from HHSC IT on all project Statements of Work (SOWs) and all IT purchases greater than or equal to \$25,000.

To ensure positive working relationships between IT and its customers, the roles and responsibilities table below contains more details.

Information Technology		Program Partner	
Role	Responsibility	Role	Responsibility
HHSC Deputy Executive Commissioner for Information Technology and Chief Information Officer (in coordination with Deputy Chief Information Officer for Governance and Deputy Chief Information Officer for IT Strategy)	<ul style="list-style-type: none"> • Manages IT resources in the best interest of the HHS system. • Final approval for IT procurements greater than or equal to \$25,000. • Highest level of escalation for customer issue resolution within IT. 	Deputy Executive Commissioner for Division	<ul style="list-style-type: none"> • Accountable for active participation in HHSC IT governance. • Accountable for compliance with policies on IT approval of any procurements of IT goods and services greater than or equal to \$25,000 originated by the customer. • Highest point of escalation for customer issue resolution within the customer agency.

Information Technology		Program Partner	
HHSC IT Directors <ul style="list-style-type: none"> • Deputy Chief Information Officer for IT Strategy • Deputy Chief Information Officer for Governance and Customer Relationship Management • Chief Information Security Officer • Director of Business Operations • Director of IT Infrastructure • Director of Application Services • Director of the Project Management Office Director of Data Center Services and Operations	<ul style="list-style-type: none"> • Accountable for delivering IT services in the assigned IT division. • Represents the interests of HHSC IT with Customer. • Point of escalation for customer issues with IT services provided within that division. 	Associate Commissioner	<ul style="list-style-type: none"> • Executive IT liaison between customer and HHSC IT. • Represents the IT interests of customer with HHSC IT. • Responsible for active participation in HHSC IT governance. • Responsible for compliance with policies on IT approval of any procurements of IT goods and services greater than or equal to \$25,000 originated by the customer. • Point of escalation for customer issues with IT services provided.
HHSC IT Management and Staff	<ul style="list-style-type: none"> • Responsible for delivering IT services within their assigned roles. • First point of escalation for customer issues with IT services provided within assigned roles. 	Deputy Associate Commissioners or as designated by the Associate Commissioner.	<ul style="list-style-type: none"> • Represents the customer agency business areas in defining and prioritizing needed IT services. • Responsible for customer feedback on IT services received. • First point of escalation for customer issues with IT services received.

SECTION 6 – Approval of Contracts for Support Services

When planning for procurements, HHS agencies and programs must receive approval from the administrative support area for any contract for a support service, or for a contract that includes the service as a component. HHS agencies and programs must also comply with requirements for approval by external entities related to contracting, as follows below.

- HHSC IT must approve all procurements and contracts for IT services, or contracts with an IT service component. Procurements and contracts may be subject to prior federal and state IT oversight approvals and reviews for compliance with information security, accessibility, and operational support requirements.
- All contracts with major IT components must include ongoing review and oversight by HHSC IT.
- Data Center Services (including software as a service, other server administration, and web site hosting) must be contracted through the State's consolidated data centers or an exemption to use another vendor must be approved by the Department of Information Resources (DIR). HHSC IT is the System's liaison with DIR.
- HHSC IT must approve contracts for IT services, or contracts with an IT service component.
- Requests for delegation to contract for external audit services must be approved by the State Auditor's Office (does not apply to consulting services).
- Requests for consulting services contracts must be approved by the Governor's Office.
- Requests to contract for outside counsel must be approved by the Office of the Attorney General.

In addition, HHS agencies and programs must provide, upon request by the support service area, reports on any contracts relating to that administrative support area from the HHS contracting system of record.

SECTION 7 – Performance Goals and Measures

Note: Section 7 is in the process of being reviewed by the Office of Transformation and Innovation (OTI) in coordination with the Office of Performance. This section will be updated with the agreed upon measures in the FY19 SSA review cycle.

SECTION 8 – Administrative Support Service by Alternative Means

As authorized by Texas Government Code Section 531.02012, Transfer and Consolidation of Administrative Support Services Functions, and detailed in Circular C-051, an HHS agency or HHSC programmatic division may request permission from the Executive Commissioner to find an alternative way of addressing an administrative

support need. If approved by the Executive Commissioner, this request would be detailed in this SECTION, as per the criteria in Circular C-051.

SECTION 9 – Staffing Implications

IT does not foresee any major changes in staffing for the division.

SECTION 10 – Performance Reporting

The HHSC administrative support area must ensure that SSA performance goals and/or measures are provided to the Executive Commissioner in annual business plan updates. Any performance issues must be raised during executive level operational briefings.

SECTION 11 – Escalation

Note: Section 11 is in the process of being updated by OTI to better support SSA issue resolution. All SSAs will be updated to include the new escalation process during this SSA review cycle

SECTION 12– Attachments

This SSA contains the following attachments:

- Attachment A – HHSC IT Application Service Levels – Descriptions of the three levels of support available for applications supported by HHSC IT.
- Attachment B – Priority Levels – Definitions of the four priority levels of application support incidents.
- Attachment C – Applications supported by HHSC IT by Portfolio - A list of applications supported by HHSC IT for use by the customer.
- Attachment D – Service Level for System-Wide Applications Supported by HHSC IT – A list of applications supported by HHSC IT for use by multiple HHS agencies.
- Attachment E – Service Level for MSS-Specific Applications Supported by HHSC IT – A list of applications supported by HHSC for use by MSS

SECTION 13 – Expiration and Modification

This agreement begins upon execution and does not have an end date. This agreement is subject to change as policies, practices, roles, and responsibilities are adjusted over time to provide optimal efficiencies and effective administrative support processes. Changes to this SSA must be agreed upon by both the support service area and the requesting or impacted HHSC division leadership prior to implementation. However, if agreement is not reached, the Executive Commissioner makes the final determination.

SECTION 14 – Points of Contact

The administrative support area and the receiving agency or program must designate points of contact for all matters related to this SSA.

HHSC Information Technology

Name: Terri Ware
Title: Director of IT Business Operations
Division: HHS IT Business Operations
Telephone Number: (512) 428-1983
E-mail: terri.ware@hhsc.state.tx.us

SSA Versions

1.	Original SSA completed	1.23.17
2.	Updated SSA - minor revisions new signatures not required	4.26.18
3.		
4.		

SECTION 15– Signature

The SSAs can be updated without routing for signature again, unless the parties do not agree on changes and/or leadership wants to sign again.

This agreement is entered into by the Parties in their capacities as stated below.

HHSC CHIEF OPERATING OFFICER

By: _____

Ruth Johnson
Chief Operating Officer

Date: _____

HEALTH AND HUMAN SERVICES COMMISSION

By: _____

Dr. Courtney N. Phillips
Executive Commissioner

Date: _____

ADDENDUM 1

HHSC IT Additional Services - Program & Services Office (CPSO)

This section includes any service additions, modifications, or deletions that are unique to an HHSC agency, division, or program, beyond the baseline services described in Section 3 or 4 of this document.

A. IT Compliance Services

A.1. Medicare Information Technology Architecture (MITA) Assessments

Service Provider:	Chief Technology Office
Description:	The MITA group will assess the business process, as well as information and technical architectures of the organization in order to update MITA maturity checklists and to prepare and distribute the MITA State Self-Assessment to Centers for Medicare and Medicaid Services (CMS).

A.2. Medicaid Managed Information System (MMIS) Certification

Service Provider:	Chief Technology Office
Description:	The MITA group will produce MITA documentation necessary for the successful completion of milestones as required by CMS in the Medicaid Enterprise Certification Toolkit.

B. IT Planning Services

B.1. MITA Architecture

Service Provider:	Data Center Services
Description:	The MITA group provides the architectural strategy and roadmap for business processes, information architecture, and technical architecture for Medicaid and other state programs in MSS. This includes a review of advance planning documents (APDs) that help ensure eligibility for Medicaid system enhanced funding, and to document compliance with the CMS Conditions and Standards.

B.2. Medicare Information Technology Architecture (MITA) Assessments

Service Provider:	Chief Technology Office
Description:	The MITA group will assess the business process, as well as information and technical architectures of the organization in order to update MITA maturity checklists and prepare and distribute the MITA State Self-Assessment to Centers for Medicare and Medicaid Services (CMS).

B.3. Medicaid Managed Information System (MMIS) Certification

Service Provider:	Chief Technology Office
Description:	The MITA group will produce MITA documentation necessary for the successful completion of milestones as required by CMS in the Medicaid Enterprise Certification Toolkit.

B.4. Interoperability Roadmap Development

Service Provider:	Chief Technology Office
Description:	Presents HHS interoperability roadmap activities to the eHealth Advisory Committee as well as other groups for feedback and, to the Health Information Executive Steering Committee for approval.

B.5. Interoperability and Standards

Service Provider:	Chief Technology Office
Description:	Engages with technical and program staff on the development of strategy, technology, procurement and project recommendations that promote the interoperability of systems that share protected health information with internal and external entities.

ATTACHMENT A - HHSC IT Application Service Levels

Service levels enable an organization to be assured of a defined amount of stability, reliability, and performance for IT applications, infrastructure and services. Service levels describe in measurable terms, the services that IT staff will furnish within a given time period.

NOTE: The service levels below are still in development. Various outsourced applications have differing definitions and levels of response time. HHSC IT is also working to document "resolution time" (time to restore application to operation) instead of "response time" (time to contact customer after incident report).

1.0 Application Availability

No.	Category	Gold	Silver	Bronze
1.1	Production	Available 24 x 7 x 365, 99.9% of the time, except for scheduled maintenance and declared disasters.	Available 24 x 7 x 365, 99% of the time, except for scheduled maintenance and declared disasters	Best Effort
1.2	Non Production Environments to include the following: <ul style="list-style-type: none"> • User Acceptance Testing • Maintenance Environment • Sandbox Environment • Training Environment 	7:00 a.m. to 6:00 p.m. Monday through Saturday and noon to 6:00 p.m. on Sunday 95% of the time except for scheduled maintenance and declared disasters.	Same	Best Effort

2.0 Application Support Services

No.	Category	Gold	Silver	Bronze
2.1	Application Support Availability (Exceptions to be approved by IT Governance at least five business days before requested special support hours.)	Monday-Friday 8:00 a.m.to 5:00 p.m. CT, excluding state-observed holidays, but will be staffed	Same	As Applicable

		on skeleton crew days.		
--	--	------------------------	--	--

3.0 Incident Management

No.	Category	Gold	Silver	Bronze
3.1	P1 (Critical) Incident Assignment Times (See Attachment B for definitions of Priority levels.)	Within normal business hours, no more than 30 minutes 99% of the time. Outside of normal business hours, no more than 60 minutes 97% of the time for P1 outages and batch processing issues requiring immediate attention.	Within normal business hours, no more than 2 hours 99% of the time. Outside of normal business hours, no more than 3 hours 97% of the time for P1 outages and batch processing issues requiring immediate attention.	Best Effort
3.2	P2 (High) Incident Assignment Times	< 2 business hours 96% of the time.	< 3 business hours 96% of the time.	
3.3	P3 (Medium) Incident Assignment Times	< 8 business hours 95% of the time.	< 16 business hours 95% of the time.	
3.4	P4 (Low) Incident Assignment Times	< 3 business days 95% of the time.	< 5 business days 95% of the time.	

4.0 Enhancements

No.	Category	Gold	Silver	Bronze
4.1	Adherence to milestone dates established through the Enhancement Scheduling Process	Target dates are met 98% of the time for all milestones established in the jointly approved work plan for an Enhancement.	Target dates are met 95% of the time for all milestones established in the jointly approved work plan for an Enhancement.	Best Effort

5.0 Service Level Reporting

No.	Category	Gold	Silver	Bronze
5.1	Monthly	No later than the 15th calendar day of each month following the end of the reporting period for the preceding month		

Notes:

The term “available” or “availability” mean the full functionality of application components hosted at SDC and ADC are available for use by authorized users.

The term “outage” means that one or more of the HHSC applications components are not available to all users for more than fifteen (15) minutes during the published hours of availability.

Planned Outage Agreements - Senior Management will be given at least 48 hours’ notice of any planned outages with estimated downtime. The notifications will be sent in the form of electronic mail.

ATTACHMENT B - Priority Levels

NOTE: These draft priority levels are still in development. Various internal and outsourced applications have differing definitions of priorities.

Priority	Characteristics
Priority 1 (P1) – Critical	<ul style="list-style-type: none">- Production outage- Production performance degradation during business hours- Critical payroll-impacting issue- Critical Security issue affecting Production Application or data- Reporting Database outage
Priority 2 (P2) – High	<ul style="list-style-type: none">- Non-critical payroll-impacting issue- Sandbox Database outage- Maintenance Database outage- Training Database outage- UAT Database outage- Sandbox performance impact- Issue impacts a large number of interfaces users and no HHSC-acceptable workaround is available- Issue is frequently occurring- Issue impacts agency compliance with federal or state law or policy
Priority 3 (P3) – Medium	<ul style="list-style-type: none">- Issue related to user acceptance testing (UAT)- Issue impacting multiple users and an HHSC acceptable workaround is available- Non-critical issues which are time sensitive (ex. file restore, missing drive mapping)- Non-impacting issue requiring additional troubleshooting and research
Priority 4 (P4) – Low	<ul style="list-style-type: none">- Issue with Workflow tasks- Issue requiring contractor to provide clarifying information

ATTACHMENT C - Applications

Supported by HHSC IT by Governance Portfolio

The objective of governance is to ensure the effective and efficient use of IT in enabling an organization to achieve its goals. HHSC IT facilitates and supports governance, a decision framework and process that allows program executives to make data-based IT investment decisions that drive business value. Governance clarifies the decision rights and accountability for both program and IT leadership roles. The governance framework will apply to key decisions regarding IT strategy, technical roadmaps, and project prioritization.

The following is the list of applications that are supported within the governance portfolios. The criticality of a system is defined as follows:

Mission Critical:

- Failure or loss of the system can contribute to death, life-threatening illness or injury for a client;
- Disruption of benefits or salary for a client or employee; or
- Result in inquiry or investigation by the media, legislature, judicial branch, SAO, LBB, or a Federal agency within 3 days or less.

Not Critical:

- Does not meet the definition of 'Mission Critical'.

Source: HHSC IT Systems Catalog (SysCat). Data as of January 4, 2019. To obtain access to SysCat, complete the Request Access to SysCat form.

Administrative Portfolio

System Name	Abbreviation	Criticalness
1099	1099	Not Critical
1099 System	1099 HHSC	Not Critical
Accounts Receivable Tracking System	ARTS	Mission Critical
Acknowledgement of Paternity	AOP	Mission Critical
Actuarial Analysis CMS Claims History	AA CMS	Mission Critical
Adverse Action Record Sharing	AARS	Not Critical
Automated Cost Reporting and Evaluation System - A	ACRES	Mission Critical
Birth Access by HHSC	HHSC Gateway	Not Critical
BRM Art Dept.	BRM_ART	Not Critical
Bugzilla	BUGZ	Not Critical
CAFM 10	CAFM 10	Mission Critical
Case Management System (DSHS)	CMS_DSHS	Not Critical
Centralized Accounting & Payroll/Personnel System Financials	CAPPS FIN	Mission Critical
Centralized Billing System	CBS	Mission Critical
Centralized Accounting & Payroll/Personnel System Human Capital Management	CAPPS HCM	Mission Critical
Chief Financial Officer Aged & Disabled DataMart	CFOD	Not Critical
Clearwell E-Discovery	Clearwell	Not Critical
Cognos Business Intelligence 10.1.1	COGNOS	Not Critical
Configuration and Change Management	CCM	Mission Critical

System Name	Abbreviation	Criticalness
Consolidated Access Control Tracking System	CACTS	Mission Critical
Correspondence Tracking System (AW)	HCTS	Not Critical
Court of Continuing Jurisdiction/Divorce	CCJ	Not Critical
DADS SharePoint On-premise	DADS SPOP	Mission Critical
Data Asset Repository	DAR	Not Critical
Disaster Assistance Payment Program	HF/DAPP	Mission Critical
Enterprise Audit Tracking System	EATS	Not Critical
Enterprise Secure File Transfer	EFT	Mission Critical
EOS	EOS	Not Critical
eTravel HHS	eTravel-HHS	Not Critical
File Manager	FileMan	Not Critical
Financial Data Warehouse	Financial Da	Not Critical
Financial Systems Data Warehouse	INFO-FSDW	Mission Critical
FSS-CFO Automated Services and Reports System	FSS-CFO	Not Critical
Grants Database	Grants DB	Not Critical
halFILE Document Imaging System	halFILE	Not Critical
HCS Provider Payment System	HCS (INFO)	Mission Critical
HHS Active Directory Forest	AD	Mission Critical
HHS Enterprise Admin Reporting and Tracking Sys	HT/HEART	Mission Critical
HHS Enterprise Portal		Mission Critical
HHS Enterprise Single Sign-On		Mission Critical
HHS File Shares		Not Critical
HHS IAM Systems Monitoring		Not Critical
HHS Insights System	HIP	Not Critical
HHS Privileged Identity Manager	PIM	Mission Critical
HHSC Forms and Print Catalog		Not Critical
HHSC IT Statistics System	HISS	Mission Critical
Historically Underutilized Business Program	HUB Portal	Mission Critical
Hospital Review System	HRS	Not Critical
HP Project and Portfolio Management	PPM	Mission Critical
IEE - Identity and Access Management	IAM	Mission Critical
iLearn	iLearn	Not Critical
Infoblox DDI	DDI	Mission Critical
Invoice Tracking System	INVTRK	Not Critical
Jitterbit		Not Critical
Legislative Tracking System (AP)	LTS-H	Mission Critical
Mail Code Lookup	Mail Code	Not Critical
Medicaid Incentive 360	MI360	Mission Critical
Office 365	O365	Not Critical
Office of General Counsel Case Management System	HL/CASE MAN	Mission Critical
Office Space	Office Space	Not Critical
One Identity Password Manager	OIPM	Not Critical
Open Records Request Tracking System	HZ/ORR	Mission Critical
OSTicketing System	OSTS	Not Critical
PaBreakdown		Mission Critical
PASRR Individual Review Monitoring	PIRM	Mission Critical
Paternity Registry	Paternity	Not Critical
Pickle COLA Multiplier	COLA	Not Critical
Position Employee Bridge for Legacy Systems	PEBLES	Mission Critical
Print Shop D-8	D-8	Not Critical

System Name	Abbreviation	Criticalness
Printer Definitions	PRTR	Mission Critical
Project and Portfolio Management	TMHP PPM	Not Critical
Project Management & Repository System	PMRS (G6)	Not Critical
Public Health Info Network - Messaging System	PHIN-MS	Not Critical
Quality Assurance and Improvement DataMart	QAI/NQ	Not Critical
Quality Assurance Fee Receivables and Collections	QAF	Mission Critical
Rate Analysis Tracking System	RATS	Mission Critical
Rate Setting Database	RSD	Mission Critical
Remedy onDemand	RoD	Not Critical
Remittance Deposition System	Remits	Mission Critical
Remote Access	RFO	Not Critical
RSA Archer eGRC	ARCH	Mission Critical
Salesforce HHS	SF HHS	Mission Critical
Send Word Now	SWN	Not Critical
SharePoint On-premises	SPOP	Mission Critical
SharePoint Online	SPO	Mission Critical
Solarwinds	Solarwinds	Not Critical
State of Texas Automated Information Reporting System	STAIRS	Mission Critical
Symantec Encryption Desktop Manager	PGP	Not Critical
System of Automated Records (JL)	SOAR	Not Critical
System of Contract Operation and Reporting	SCOR	Mission Critical
Systems Catalog	SysCat	Mission Critical
Tanium		Not Critical
TEAMMATE	TEAMMATE	Mission Critical
Texas Primary Care Office	TPCO	Not Critical
TIERS Historical Case Report	THCR	Not Critical
USAS Report Handler	USASREPT	Not Critical
Verint Workforce Optimization	WFO	Mission Critical
Video Conference Registration	VCRreg	Not Critical
Voluntary Adoption Registry	VAR	Not Critical
Web Random Moment Sampling	Web RMS	Not Critical
Weekly Report Entry	WREN	Not Critical
WIC Adobe Connect		Not Critical
Work Measurement Data Collection Tablet System	WMDCS	Not Critical

Health and Specialty Care System Portfolio

System Name	Abbreviation	Criticalness
Activity Tracker - Abilene	AT - Abilene	Mission Critical
Activity Tracker - Austin	AT - Austin	Mission Critical
Activity Tracker - Brenham	AT - Brenham	Mission Critical
Activity Tracker - Corpus Christi	AT - Corpus	Mission Critical
Activity Tracker - Denton	AT - Denton	Mission Critical
Activity Tracker - Lubbock	AT - Lubbock	Mission Critical
Activity Tracker - Lufkin	AT - Lufkin	Mission Critical
Activity Tracker - San Angelo	AT - San Ang	Mission Critical
Activity Tracker - San Antonio	AT - San Anto	Mission Critical
Activity Tracker- Richmond	AT-Richmond	Mission Critical
Annual Hospital Survey System	AHSS	Not Critical
Client Abuse & Neglect Reporting System	CANRS	Mission Critical

System Name	Abbreviation	Criticalness
Client Assignment & Registration System	CARE	Mission Critical
Client Trust Fund	CTF	Mission Critical
Driving Records Request System	DRRS	Not Critical
DSHS Sage Fundraising 50	SAGE	Not Critical
IMDMSIS Claims Processing	IMDMSIS	Not Critical
Integrated Resident Information System	IRIS	Mission Critical
Materials Inventory Management System	MIMS	Mission Critical
MediMAR	MediMAR	Mission Critical
myAvatar	myAvatar	Mission Critical
Practice Partner Patient Records	EMR	Mission Critical
Practice Partner Scheduling	PPART	Mission Critical
Quality Services Oversight for Clinical Performance	QSO-CPI	Not Critical
Quality Services Oversight for Facility Support	QSO-FSPI	Not Critical
Sunquest Healthcare Laboratory System	Sunquest	Mission Critical
WORx Drug Therapy Management System	WORx	Mission Critical
X-Porter Delivery System	JHSXPTR	Mission Critical

Inspector General Portfolio

System Name	Abbreviation	Criticalness
Automated System for the Office of Inspector General	JD/ASOIG	Mission Critical
BASS Request System		Not Critical
Document Storage for Tracking Internal Affairs Cases		Not Critical
Hospital Utilization Review System	HURS	Mission Critical
Hotline Inquiry		Mission Critical
IG Portal (Internal & External)		Not Critical
MCO/SIU Case Tracker	MCOSIU	Not Critical
Medicaid Fraud and Abuse Detection System (MFADS)	MFADS	Mission Critical
Nursing Facility Utilization Review	NFUR	Mission Critical
OIG Time Keeper		Not Critical
OIG Utilization Review -OIE - TILE/CBA Trng Data	OIG-TRN	Not Critical
Payment Authorization Tracking System	PATS	Not Critical
Personnel Action Form	PAF	Not Critical
Position Tracking System	PTS	Mission Critical
Provider Enrollment Tracking System	PETS	Not Critical
Strategic Operations & Professional Development	SOPD	Not Critical
Texas Exclusions Database		Not Critical
Waste, Abuse and Fraud Referrals System	WAFERS	Mission Critical

Medical and Social Services Portfolio - Access & Eligibility Services Sub Portfolio

System Name	Abbreviation	Criticalness
2-1-1 Internet System (G2)	2/1/2001	Not Critical
Admin Application Management for Service Authorization Online	ADAM	Mission Critical
Audit Trail		Not Critical
Buy-In and Part-A Payor	MF	Mission Critical
Claims Management System - Service Authorizations	MG/CMS-SAS	Mission Critical
Community Care Aged/Disability Caseload Realignment	HX/CCAD	Mission Critical
Community Care Case Reading System	CC-CRS/JR	Mission Critical

System Name	Abbreviation	Criticalness
Comprehensive Interest List for Long Term Care Services	HY/CCSIL	Mission Critical
DADS Admin Tool	DAT	Not Critical
DADS WorkCenter	Work Center	Mission Critical
Data Broker System	DBS	Mission Critical
DataMart for EA Reporting		Not Critical
EBT Data Storage and Retrieval System	HE/EBT	Not Critical
Eligibility Determination & Notification	EDEN	Mission Critical
Eligibility Services Portal	ESPortal	Not Critical
Eligibility Workload Management System	EWMS	Mission Critical
Harmony	Harmony	Mission Critical
Hospice Batch Forms	xBatch	Not Critical
Lifeline and Electric Utilities Program	PT TEL-ASSIS	Not Critical
Long Term Care (LTC) Search	LTC Search	Not Critical
Long Term Care Case Scheduler	LTCCS	Mission Critical
Long Term Care Services Intake System	JN/NTK	Mission Critical
LTC Provider System	NE	Mission Critical
MEPD	MEPD	Mission Critical
Presumptive Eligibility Website	PE	Not Critical
Program Area Learning Management System (PALMS)	PALMS	Not Critical
SAVERR Purged Data Inquiry System	SPDIS	Not Critical
Self Service Portal	SSP	Mission Critical
Social Security Administration Online Query	HK SSA ONLIN	Not Critical
State Portal	STP	Mission Critical
State Unit on Aging Information Management System	SPURS IMS	Mission Critical
Texas Integrated Eligibility Redesign System	TIERS	Mission Critical
TZ TWC TWIST	TZ	Not Critical
Wired Third Party Query	NB WTPY	Not Critical

Medical and Social Services Portfolio - Health, Developmental & Independence Services Sub Portfolio

System Name	Abbreviation	Criticalness
Autism		Mission Critical
Board Evaluation of Interpreters	BEI	Mission Critical
Community Health Clinic Locator	CHCL	Not Critical
CRS Post-Acute Rehabilitation Services Data Report	CRS	Mission Critical
Early Intervention Specialist Registry	EIS Registry	Mission Critical
ECI Reporting System	ECI-REP	Mission Critical
Family Violence System	FAMV	Not Critical
Guardianship Online Database	GOLD	Mission Critical
Independent Living Services Data Reporting System	ILS	Mission Critical
Integrated Business Information System	IBIS	Mission Critical
Med-IT Breast & Cervical Cancer	Med-IT	Mission Critical
STAP Telephone Assistance	STAP-TA	Mission Critical
Surrogate Decision Making	SDM	Mission Critical
Texas Kids Intervention	TKIDS1	Mission Critical
Texas WIC Information Network	TXWIN	Mission Critical
Texas WIC Information Network - EBT	EBT-WIN	Mission Critical
Texas WIC Information Network - TXIN	TXIN	Mission Critical
Texas WIC IT Help Desk Remedy Ticket System	HD Remedy	Mission Critical

System Name	Abbreviation	Criticalness
Texas WIC Warehouse Inventory Management Sys	WIMS	Not Critical
Twogether In Texas	TwoIT	Not Critical
WIC Web Applications	WICWeb	Not Critical

Medical and Social Services Portfolio - Intellectual and Developmental Disabilities & Behavioral Health Services Sub Portfolio

System Name	Abbreviation	Criticalness
Clinical Management for Behavioral Health Services	CMBHS	Mission Critical
CMS ICF/MR Provider Payment System	ARSP-CMS	Mission Critical
DSHS Contracting System AKA Source.net	Source.net	Mission Critical
Mental Retardation and Behavioral Health Outpatient	MBOW	Mission Critical
MR CARE	CARE/RI	Mission Critical
Query Reporting System	QRS	Mission Critical

Medical and Social Services Portfolio - Medicaid & CHIP Services Sub Portfolio

System Name	Abbreviation	Criticalness
Business Objects	Bus. Obj.	Mission Critical
Children and Pregnant Women	CPW	Not Critical
Claims II System	Claims II	Mission Critical
Client Automated Information Tracking System	CAITS	Not Critical
Code Table Automation	CTA	Not Critical
Compass 21	Compass21	Mission Critical
Delivery Supplemental Payment Processing	DSPP	Mission Critical
Delivery System Reform Incentive Payment Program	DSRIP	Not Critical
Electronic Data Interchange	EDI2	Mission Critical
Enrollment Broker Financial Application	MAXeb Finance	Mission Critical
Lobby PC Kiosk - Dynatouch (TIPS)	KIOSK	Not Critical
Long Term Care Online Portal	LTC Portal	Mission Critical
MAXDat Reporting	MAXDat	Mission Critical
MAXeb	MAXeb	Mission Critical
Medicaid Buy-in for Children Program	MBIC	Mission Critical
Medicaid Contract Administration Tracking	MCATS	Mission Critical
Medicaid Identification Cards System	MED ID	Mission Critical
Medicaid Management Information System	MMIS	Mission Critical
Medicaid/CHIP Policy Auto Tracking System-DG	McPAT	Mission Critical
OnBase	OnBase	Not Critical
Portal - TMHP.com	WWW	Mission Critical
Premiums Payable System	MA	Mission Critical
Prior Authorization on the Portal	PA on Portal	Mission Critical
Provider Recoupment & Hold Desktop	PRH Desktop	Not Critical
Quality Monitoring Visit	QMVisit	Not Critical
Texas Health Steps	MP/THSteps	Not Critical
Texas Inventory of Respite Services	TIRS	Not Critical
Texas Medical Transportation System	TMTS	Mission Critical
Texas Vendor Drug Program website		Not Critical
Third Party Liability/Third Party Recovery	TPL/TARS	Mission Critical
Third Party Resources	TPR / TS	Mission Critical
Transformed-Medicaid Statistical Information System	T-MSIS	Mission Critical

System Name	Abbreviation	Criticalness
Vision 21	V21	Mission Critical

Medical and Social Services - Other

System Name	Abbreviation	Criticalness
Disability Determination Services	DDS	Not Critical

Public Health Services Portfolio

System Name	Abbreviation	Criticalness
Adoption	Adoption	Mission Critical
Affidavit Request for Exemption from Immunizations	COREQUEST	Not Critical
AIDS Regional Information Evaluation System(ARIES)	ARIES	Not Critical
Birth Certificate Abstract Print	PRS Print	Not Critical
Birth Issuance History	Issuance	Not Critical
Certificate Numbering	Cert Number	Not Critical
Child Health Reporting System	CHRS	Not Critical
Cluster Request Database	CRD	Not Critical
Combined Perinatal HepB Mother/Infant Registry	HBM/HBC	Not Critical
Contship	CSHIP	Not Critical
Dangerous Wild Animals Registration	DWA	Not Critical
Dovico Timesheet	Timesheet	Not Critical
Electronic HIV/AIDS Reporting System (EHARS)	eHARS	Not Critical
Electronic Laboratory Exchange Network (eLEXNET)	eLEXNET	Not Critical
Enrollment Broker Self Service Portal	EBSSP	Mission Critical
Executive & Staff Operations Information Center	ESO IC	Not Critical
FIC	FIC	Not Critical
Hansen's Disease Registry	Hansen	Not Critical
Harvest	Harvest	Not Critical
Health Care Data Collection System	HCDCS	Not Critical
Health Registries - Birth Defects Registry	BDR	Not Critical
Health Registries - Child/Adult Blood Lead Epi and Survey	CABLES	Not Critical
Health Registries - Trauma Registry	TraumaReg	Not Critical
Health Registries - TX Healthcare Safety Network	TxHSN	Not Critical
HealthPac	HealthPac	Not Critical
Immunization Clinic Database	ICD	Not Critical
Immunization Communication & Training Customer DB	CAT	Not Critical
Inventory Tracking Electronic Management System	ITEAMS	Mission Critical
LabWare	PHLIMS	Mission Critical
Labworks	Labworks	Not Critical
National Electronic Disease Surveillance System	NEDSS	Mission Critical
Newborn Screening (NBS) Laboratory (LIMS)	SpecimenGate	Mission Critical
Nursing Licensure Dbase	MS ACCESS	Not Critical
Poison Control Network Centralized Database	PCN	Not Critical
Publications	PUBS	Not Critical
Quality Fee Pull	Quality	Not Critical
Rabies Biologicals Distributed by DSHS	RB	Not Critical
Records	Records	Not Critical
Registry Plus		Not Critical
Remote Site Billing	Billing	Not Critical

System Name	Abbreviation	Criticalness
Results Web Portal	Web Portal	Not Critical
SEER*Stat	SEER*Stat	Not Critical
Sensaphone Monitoring System	SMS	Mission Critical
Sexually Transmitted Disease Mgmt Info System	STD*MIS	Not Critical
SSA Birth Transmittal File Data Filter	SSA To	Not Critical
Syndromic Surveillance	TxS2	Not Critical
TB and Infection Control Surveillance Database	Paradox	Mission Critical
TB, HIV, & STD Integrated System	THISIS	Not Critical
Texas Electronic Registrar	TER	Mission Critical
Texas Health Data (new)	THD	Not Critical
Texas HIV Medications Program System	HIV2000	Mission Critical
Texas Immunization Registry 2	ImmTrac2	Not Critical
Texas RedSky	TxRedSky	Not Critical
Texas Vendor Drug Program Pharmacy System	OS+	Mission Critical
Texas-Wide Integrated Client Encounter System (TWI	TWICES	Not Critical
Vision and Hearing Screening Certified Instructors	VHCERTINSTS	Not Critical
Vital Statistics Unit County Contacts	VSU CC	Not Critical
VitalNet	Vitalnet	Not Critical
VSS FileNet Domain Controllers	VSS FileNet	Mission Critical
Web Content Management System	WCMS	Not Critical
Zoonosis Surveillance Database	ZCDSURV	Not Critical

Regulatory Services Portfolio

System Name	Abbreviation	Criticalness
Abuse, Neglect and Exploitation Database & Report	ANE	Mission Critical
Agency Records Management Systems	ARMS	Mission Critical
Aspen Central Office	HW / ASPEN	Mission Critical
BLC Federal HFL Compliant System	ASPEN	Not Critical
Central Data Repository	CDR	Mission Critical
Childcare Licensing Automated Support System	CLASS	Mission Critical
CLASSMate		Not Critical
Credentialing Manager	Cred Mgr	Not Critical
Early Warning System Data Mart	EWS	Not Critical
Employee Misconduct Registry	EMCR	Mission Critical
Employee Misconduct Registry Tracking Tool	EMR Track	Mission Critical
Medicaid Occupancy Report	MORT	Not Critical
Minimum Data Set	NZ / MDS	Mission Critical
Nurse Aide/Medication Aide Referral Tracking		Not Critical
Nursing Facility Administrators System	NT / NFA	Mission Critical
Outcome and Assessment Information Data Set Manage	OASIS	Not Critical
Public and Provider	PP	Mission Critical
Radiological Monitoring Instrument Tracking	KIT	Not Critical
Regulatory Automation System	RAS	Mission Critical
To Help our Reviewers THOR	THOR	Not Critical
Waiver Survey and Certification Residential Review	WSC	Not Critical
Web Incident Portal		Mission Critical

ATTACHMENT D - Service Level of System-Wide Applications Supported by HHSC IT

Application	Service Level
Adverse Action Record Sharing (AARS)	Silver
ARTS	Gold
CAPPS HR	Gold
Client Trust Fund (CTF)	Silver
On-line Electronic Travel System (HHS eTravel)	Silver
Financial Data Warehouse (FSE)	Gold
HCATS	Silver
HHS Electronic Automated Records Tracking (HEART)	Silver
HHSAS Financials	Gold
HHS Legislative Tracking System (HLTS)	Gold
MCATS	Silver
Internet Learning System (iLearn)	Silver
Project Management Repository System (PMRS)	Silver

ATTACHMENT E - Service Level for MSS Division-Specific Applications

Supported by HHSC IT Division

Application	Program Area	Service Level
2-1-1 IVR	Eligibility	Silver
AskIT Knowledgebase	Eligibility	Silver
Autism	Health, Developmental & Independence Services	Silver
Board of Evaluation of Interpreters (BEI)	Health, Developmental & Independence Services	Silver
CAFM	Transferring DADS Programs State Hospitals and State Supported Living Centers	Bronze
Call Center Inquiry (CCI)	Eligibility	Gold
Community Resource Coordination Groups (CRCG) website	Eligibility	Silver
Comprehensive Rehabilitation Services (CRS) Post-Acute Rehabilitation Services Data Reporting System (Deployed 9/6/2016)	Health, Developmental & Independence Services - Rehabilitative & Independence Services	Gold
Data Mart	Eligibility	Gold
Document Center	Eligibility	Gold
Early Intervention Specialist (EIS) Registry	Health, Developmental & Independence Services - Early Childhood Intervention Administration	Gold
EBT Archive (Data Storage & Retrieval System)	Eligibility	Bronze
ECI Reporting System (Financials)	Health, Developmental & Independence Services - Early Childhood Intervention Administration	Silver
Enterprise Content Management (ECM)	Eligibility	Gold
Family Violence (FVNET)	Eligibility	Silver
Grandparent Payment System (GPS)	Eligibility	Bronze
Independent Living Services Data Reporting System (Deployed 9/6/2016)	Health, Developmental & Independence Services	Gold

Application	Program Area	Service Level
ITS (Integrated Tracking System for Family Violence)	Eligibility	Silver
Kofax*	Eligibility	Gold
Long Term Services & Supports (LTSS)	Eligibility	Gold
Med ID	Medicaid	Silver
Medicaid Buy-In (MBI)	Medicaid	Silver
Medicare Buy In (A&B)	Medicaid	Silver
Premiums Payable System (PPS)	Medicaid	Gold
Refugee Data Collection (RDC)	Eligibility	Silver
SPDIS	Eligibility	Silver
Specialized Telecommunication Assistance Program (STAP) - Program Managed until 5/2017	Health, Developmental & Independence Services	Silver
State Portal (STP)	Eligibility	Gold
Task List Manager (TLM)	Eligibility	Gold
Texas Kids Intervention (TKIDS)	Health, Developmental & Independence Services - Early Childhood Intervention Administration	Gold
Texas Medical Transportation System (TMTS)	Medicaid - MTP	Gold
TIERS	Eligibility	Gold
TMSIS Medicaid Eligibility	Medicaid	Silver
TRAD (ECI)	Health, Developmental & Independence Services	Silver
WFM - Scheduler	Eligibility	Gold
Wired Third Party Query System (WTPY)	Eligibility	Silver

Application	Program Area	Service Level
Workflow Management (WFM)	Eligibility	Gold
yourtexasbenefits.com	Eligibility	Gold
YTB mobile app	Eligibility	Gold
Caseload Realign (SASO ADMIN)	Eligibility - Community Services & Program Operations	Gold
Client Record System (CRS)	State Supported Living Centers	Gold
CMS Merge (SASO ADMIN)	Eligibility - Community Services & Program Operations	Gold
Code Table Automations	Medicaid - Claims Support Services	Gold
COGNOS	HHSC Budget	Gold
Community Care Case Reading System (CCCRS)	Eligibility - Community Services & Program Operations	Gold
Community Services Interest List (CSIL)	Eligibility	Gold
Compliance, Assessment, and Regulatory Enforcement System (CARES)	Regulatory Services	Gold
DADS Reports	Eligibility	Gold
DADS WorkCenter	Eligibility	Gold
Eden Services	Eligibility - Community Services & Program Operations	Gold
ID CARE - Money Follows the Person - Finder File and File Delivery to CMS	Intellectual and Developmental Disabilities & Behavioral Health Services	Gold
ID CARE - Overall	Intellectual and Developmental Disabilities & Behavioral Health Services	Gold
JIRA SLOT Tracking (SASO ADMIN)	Eligibility - Community Services & Program Operations	Gold
Long Term Care Services Intake System (NTK)	Eligibility - Community Services & Program Operations	Gold
LTC Datamart	CFO	Gold
LTC Provider System (NE)	Transferring DADS Programs	Gold

Application	Program Area	Service Level
Medically Dependent Children Program (MDCP) Limited Stay (Salesforce)	Eligibility - Community Services & Program Operations	Silver
Mental Retardation Behavioral Health Outpatient Warehouse (MBOW)	Intellectual and Developmental Disabilities & Behavioral Health Services	Bronze
Notifications (SASO ADMIN)	Eligibility - Community Services & Program Operations	Gold
PEBLES	HHSC Budget	Silver
Promoting Independence	Intellectual and Developmental Disabilities & Behavioral Health Services	Gold
Provider System (NE Batch)	Community Service Contracts	Gold
Quality Assurance& Improvement (QAI) Data Mart	CADS - Aging & Disability	Silver
Texas Inventory of Respite Services	Community Access and Grants	Silver
SAS (MG Batch)	Eligibility - Community Services & Program Operations	Gold
Scheduler (SASO ADMIN)	Eligibility - Community Services & Program Operations	Gold
Service Authorization System (SAS)	Eligibility - Community Services & Program Operations	Gold
Service Authorization System Online (SASO Wizards)	Eligibility - Community Services & Program Operations	Gold
SLOT Tracking	Eligibility - Community Services & Program Operations	Gold
Surrogate Decision Making	Health, Developmental & Independence Services - Guardianship Services	Gold
UniGateway	Eligibility - Community Services & Program Operations	Silver
Utilization Review	Medicaid	Silver
Children and Pregnant Women (CPW)	Medicaid	Gold
Clinical Management for Behavioral Health Services (CMBHS)	Intellectual and Developmental Disabilities & Behavioral Health Services	Gold
DSHS Contracting System (Source.net)	Intellectual and Developmental Disabilities & Behavioral Health Services	Gold
Family & Community Health Services Clinic Locator (CHCL)	Health, Developmental & Independence Services	Gold

Application	Program Area	Service Level
Institution for Mental Diseases - Medicaid Statistical Information System (IMD-MSIS)	Medicaid	Gold
Integrated Business Information System (IBIS)	Health, Developmental & Independence Services	Gold
Practice Partner	Rio Grande State Hospital	Gold

Exhibit I: 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

P. O. Box 13247 • Austin, Texas 78711 • 4900 North Lamar, Austin, Texas: 78751 • 512-424-6500

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 J: 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 <input type="text"/>	
* PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	
Prefix: <input type="text"/>	* First Name: <input type="text"/> Middle Name: <input type="text"/>
* Last Name: <input type="text"/>	Suffix: <input type="text"/>
* Title: <input type="text"/>	
* SIGNATURE: <input type="text"/>	* DATE: <input type="text"/>

Exhibit K: Federal Assurances

ASSURANCES - NON-CONSTRUCTION PROGRAMS

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

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

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

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

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.
2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.
3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.
4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.
5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).
6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.
7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.
8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§275a to 275a-7), the Copeland Act (40 U.S.C. §275c 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