ADMINISTRATION FOR
CHILDREN & FAMILIES
Office of the Chief Information Officer

ACF Security, Privacy and Task Standard Language for Acquisitions

ACF OCIO

Version 1.0

ADMINISTRATION FOR
CHILDREN & FAMILIES
Office of the Chief Information Officer

Dated 12/18/2019

Revision History

Date	Version	Remarks
12/18/2019	1.0	Implementation of Standard Security, Privacy and Task SOW Language

Table of Contents

1. Purpose

The Standard Security, Privacy and Task language is designed to provide ACF with a baseline set of requirements and task language to be used in its procurements. Specifically, procurements involving IT services or access to personally identifiable information (PII) or Federal IT systems.

2. IT Security Requirements

A. Baseline Security Requirements

1) **Applicability.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information as required to perform their work. Access is contingent upon positive adjudication of background check.

b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the ACF mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

2) **Safeguarding Information and Information Systems.** In accordance with the Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:

a. Protect government information and information systems in order to ensure:

- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
- **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
- **Availability**, which means ensuring timely and reliable access to and use of information.

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of ACF regardless of location.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract.

d. Comply with the Privacy Act requirements and tailor FAR clauses as needed.

3) **Information Security Categorization**. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categorie*s, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system. The contractor shall work with the ACF security team to categorize information or information systems. The categorization can change at any time throughout the lifecycle of the system. The contractor shall ensure proper controls are implemented based on the categorization.

4) **Controlled Unclassified Information (CUI).** CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "h*andling"* refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

a. marked appropriately;

b. disclosed to authorized personnel on a Need-To-Know basis;

c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and

d. returned to ACF control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.

5) **Protection of Sensitive Information**. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

6) **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by ACF or collected by the contractor on behalf of ACF shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any ACF records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS and ACF policies. Unauthorized disclosure of information will be subject to the HHS/ACF sanction policies and/or governed by the following laws and regulations:

a. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
b. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
c. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

7) **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.

8) **Websites and Digital Services.** All new and existing public-facing government websites shall comply with the Integrated Digital Experience Act (IDEA).

9) **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

9) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents, if applicable, to comply with contract deliverables as appropriate.

10) **Standard for Encryption.** The Contractor (and/or any subcontractor) shall:

a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.

b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and ACF-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR prior to implementation of the solution.

e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11) **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the

ACF non-disclosure agreement. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – When applicable, the Contractor shall assist the ACF Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the ACF SOP or designee with completing a PIA for the system or information within *30 days* after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

b. The Contractor shall assist the ACF SOP or designee in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

B. Training

1) **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/ACF Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete HHS/ACF Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training shall be compliant with HHS training policies.

2) **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

3) **Training Records.** The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records shall be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

C. Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*.

2) All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual ACF Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines.

D. Incident Response

FISMA defines an incident as “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Contractor (and/or any subcontractor) shall comply with ACF’s Incident Response Policy dated July 10, 2018, including any subsequent updates.

In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1) Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident.

2) Notify affected individuals only as instructed by the Contracting Officer or designated representative.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the ACF Incident Response Team (IRT), COR, CO, ACF SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic as defined in ACF’s Incident Response Policy.

4) Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

E. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

[insert position sensitivity designation levels based on OPM’s Position Sensitivity Designation Tool]

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within 3 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 24 hours of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

F. Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

The Contractor (and/or any subcontractor) and its employees shall comply with computing and security standards including:

- Federal Information Security Management Act (FISMA) as part of the e-government Act of 2002
- Homeland Security Presidential Directive (HSPD)-12,
- Policy for a Common Identification Standard for Federal Employees and Contractors;
- Office of Management and Budget (OMB) Memorandum (M)05-24; and
- Federal Information Processing Standards Publication (FIPS PUB) Number 201,
- FAR Subpart 4.13 (https://acquisition.gov/sites/default/files/current/far/compiled_html/subpart_4.13.html),
- FAR Subpart 52.204-9 (https://www.acquisition.gov/?q=browsefar), and
- HHS HSPD-12 policy

The Contractor shall refer to the HHS-OCIO Policy for Information Systems Security and Privacy, dated July 7, 2011. The Contractor shall become familiar with the HHS Departmental Information Security Policies, which may be found at https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html. The HHS Cybersecurity Program develops policies, procedures, and guidance to serve as a foundation for the HHS information security program. These documents implement relevant Federal laws, regulations, standards, and guidelines that provide a basis for the information security program at the Department. The Contractor must become familiar with HHS Cybersecurity Program guidelines as presented at https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/information-security-privacy-program/index.html.

G. Contract Initiation and Expiration

1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Solution Development Life Cycle (SDLC) processes, ACF Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the ACF SDLC framework and methodology.

2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

3) **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are

appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 48 hours before an employee stops working under this contract.

5) **Contractor Responsibilities Upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or ACF policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the **ACF** Contractor Employee Separation Checklist when an employee terminates work under this contract within 3 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. Records Management and Retention

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/ACF policies and shall not dispose of any records unless authorized by HHS/ACF.

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/ACF policies.

3. Hosting of a Federal IT System

The contractor shall provide the hosting facility for related support services to accommodate ACF's production, test, development, staging, training, and all other environments for the **O**PRE **P**ortfolio Management **S**ystem (OPS). The Contractor shall ensure that the host facility and systems installed meet HHS and ACF security standards provided in the IT Security Requirements section and are able to receive and maintain an authority to operate (ATO). In addition, the contractor shall ensure cloud solutions are FedRAMP approved. Representative tasks may include, but are not limited to:

- Website hosting
- Infrastructure support
- Communications
- Network interfaces
- Enhancements and other maintenance
- Data backup and recovery

Hosting and Administration involves providing the information technology (IT) infrastructure (facilities and infrastructure software) that serve as the foundation for running business software applications and the services to maintain that infrastructure. The contractor will provide all the necessary services to support and host the solution, consistent with the goals and objectives of this SOW. This includes both infrastructure hosting and application functional and technical support.

The contractor is expected to provide a complete hosting solution that includes all the services necessary to deliver their proposed approach from project initiation through system cut-over and all post-deployment production operations.

Security Requirements for GOCO and COCO Resources

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*; *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and* Organizations; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

2) **Security Assessment and Authorization (SA&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s). The ATO timeline/schedule shall be determined within 30 days of contract award and approved by the ACF OCIO. The Contractor shall conduct the SA&A requirements in accordance with *HHS IS2P/*, NIST SP 80037, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

ACF's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

a. SA&A Package Deliverables -The Contractor (and/or any subcontractor) shall provide a SA&A package, within *the timeframes listed below,* to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package:

- **System Security Plan (SSP)** – due date to be determined and approved by the ACF OCIO after contract award and in accordance with the ATO schedule. The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and ACF policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It

should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least ***annually*** thereafter.

- **Security Assessment Plan/Report (SAP/SAR)** – due date to be determined and approved by the ACF OCIO after contract award and in accordance with the ATO schedule. The security assessment shall be conducted by *the* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and ACF policies. The assessor will document the assessment results in the SAR.

- **Interconnection Security Agreement (ISA)** – due date to be determined and approved by the ACF OCIO after contract award and in accordance with the ATO schedule. The contractor will submit a current agreement or complete an ISA with ACF to document interconnection arrangements and information security responsibilities for both parties, including an outline of security safeguards, and technical and operational security requirements based on the National Institute of Standards and Technology (NIST) Security Guide for Interconnecting Information Technology Systems (Special Publication (SP) 800-47 http://csrc.nist.gov/piblications/nistpubs/800-47/sp800-47.pdt) and shall comply with the security required by Federal Acquisition Regulation (FAR) clause 52.239-1, Privacy or Security Safeguards.

Thereafter, the Contractor, in coordination with **ACF** shall conduct and assist in the assessment of the security controls and update the SAR at least ***annually.***

- **POA&M** – due date to be determined and approved by the ACF OCIO after contract award and in accordance with the ATO schedule. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and ACF policies. All high-risk weaknesses must be mitigated within 30 days and all medium weaknesses must be mitigated within 60 days from the date the weaknesses are formally identified and documented. ACF will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, **ACF** may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated on a real-time basis as vulnerabilities are discovered. The POA&M shall be reported to ACF OCIO quarterly.

- **Contingency Plan and Contingency Plan Test** – due date to be determined and approved by ACF OCIO after contract award and in accordance with the ATO schedule. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and ACF policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least ***annually***.

- **E-Authentication Questionnaire** – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication*

Guidelines. Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS policies.

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/Pen Test -**Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates 14 days of the assessment or test.

- **Asset Management -** Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least 30 days prior to deployment. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

- **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least 30 days before deployment. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

- **Vulnerability Management -** Use SCAP-compliant automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least monthly.

- **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an

expedited manner, within vendor and agency specified timeframes, at least, within 14 days for critical, 30 days for high, 60 days for medium, 90 days for low from the release date of patch.

- **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

- **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

3) **Government Access for Security Assessment**. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:

a. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

c. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

d. Cooperate with inspections, audits, investigations, and reviews.

4) **End of Life Compliance.** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO). The contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS *End-of-Life Operating Systems, Software, and Applications Policy*.

5) **Servers, Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of ACF are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

a. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with ACF encryption standards;

b. Ensure end user devices do not store or process data outside of an IT system;

c. Maintain the latest operating system patch release and anti-virus software definitions within 14 days for critical, 30 days for high, 60 days for medium, 90 days for low from the release date of patch;

d. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

- Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

- Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a ***monthly*** basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

4. Operations and Maintenance for a Federal IT System

The Contractor shall monitor, manage, assess, and report on the OPS. Operations and maintenance on IT systems shall include all software and hardware associated with client/servers, web-based applications and networks. This support shall include both major and minor releases. This includes deployment planning, deployment support, support or promoting the release to the pre-production and production environments, and associated documentation. Representative activities include, but are not limited to:

- Operational Support Software Maintenance and Upgrades
- Infrastructure Management

- IT Optimization
- Help Desk/IT Support
- Client server and network monitoring;
- Virtual Private Network (VPN) with secure remote access;
- Server configuration and provisioning services; server management;
- Managed firewall; information security services;
- Service Level Agreements (SLAs) are maintained based upon ACF's requirements and approved by the COR

The Contractor shall perform ongoing operations and maintenance support for the OPS. Specifically, the tasks shall include but is not limited to: application enhancement, help desk support, system integration, implementation, testing and training. All tasks shall be performed in accordance with ACF's Software Development Life Cycle (SDLC). The Contractor shall update or develop user documentation, system documentation, release notes, and ACF SDLC documentation as necessary to ensure that documentation is current. The Contractor shall cooperate, collaborate, and participate as part of team to implement enhancements when other vendors are included.

Disaster Recovery and Continuity of Operations

As tasked, the Contractor shall implement redundant and/or disaster recovery sites. Representative activities include, but or not limited to the following:

- Develop plans for redundant site
- Setup redundant site
- Operate and maintain redundant site
- Develop Disaster Recovery Plan
- Setup Disaster Recovery Site
- Operate and maintain Disaster Recovery Site
- Conduct periodic Disaster Recovery Tests
- Conduct Annual Failover testing of the DR site to ensure compliance with IT security standards
- Provide a separate Disaster Recovery Hosting Facility Site located in a different geographical region of the country and approved by the COR, as required by the ACF OCIO
- Prepare and maintain documentation required for Authority to Operate, system backup and recovery, system security plan, and other documentation related to the operations and maintenance of the hosted recovery site.

The Contractor shall ensure that the hosting environment is compliant with the National Institute of Standards and Technology (NIST)' Information Security Continuous Monitoring for Federal Information Systems and Organizations and Federal Information Security Management Act (FISMA).

Change Management

The Contractor shall implement an end-to-end change management service for the OPS. The Contractor shall:

- Define, document, implement, and enforce integrated change control and service desk services that establish controlled processes for managing change in the computing environments. This would include the implementation of change management tools to track, schedule, and report on all change activities.
- Participate in Production Change Control Board (PCCB) meetings to discuss change management and program management issues.

The Contractor shall implement a change management capability for all changes to computing resources and service assets in the computing environment. The Contractor shall be responsible for implementing a change management system (CMS) and processes that capture changes and related impacts of all applications, processes affecting ACF computing. The Change management process shall provide automated validation reporting of configurations violations where possible.

The CMS shall provide the capability to restore computing resource configuration violations to their valid state. The CMS shall track all hardware and software configuration items (CI) throughout the lifecycle of a change as well as licenses to ensure fully functioning and license agreements are renewed on a timely basis. The configuration process shall provide the government with a request for new hardware and software license purchases at least 15 business days prior to the need for approval and/or expiration date of a license agreement.

The CMS shall include tools for collecting, storing, managing, updating, analyzing, and presenting data about all CIs. The data from the tools that support the CMS shall be available to the Government with online graphical user interfaces and dashboard formats with near real-time information. The data from the CMS will be used in the quarterly reporting in support of the following:

- Demand and Capacity Management Planning
- Technical Management
- Schedule Management
- Cost Management
- Resource Management
- Communication Management

5. Data Rights (Include in Section H.)

Data Rights

The Government has unlimited rights to all documents/material produced under this task order. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of the ownership/copyright belonging exclusively to the Government. These documents and materials

may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. The right does not abrogate any other Government rights under the applicable Data Rights clause(s).

All data collected by the Contractor or provided to the Contractor in the performance of this contract are the property of the Government. The Government retains all rights to the data used and all derivative works developed by the Contractor. The Contractor agrees that during performance of the contract and for a period of six (6) years after the completion of performance of this contract, the Contractor, including all divisions thereof, and any affiliate of the Contractor, any joint venture involving the Contractor, any entity into or with which it may subsequently merge or affiliate, or any other successor or assign of the Contractor, shall not:

- Supply information or material received from this contract, to the public or to any firm participating in or having a known prospective interest in the subject matter areas for which the sensitive information such as the name or mission of the government agency/department that provided the data was initially submitted.

6. Project Management

Project Management Plan

The Contractor shall develop maintain and update a Project Management Plan (PMP). The PMP shall provide the basis for performing and controlling the project's activities in accordance with the Task Order. This document describes the technical approach, organizational resources, deliverables, documentation, and management controls to be employed to meet the cost, performance, and schedule requirements throughout the Task Order period of performance.

These management activities shall establish control, management, monitoring, and notification mechanisms and shall include working with and reporting to the ACF COR to ensure that tasks and their subtasks stay on track and important milestones are met. Representative activities include, but are not limited to:

- Plan, organize, secure, and manage resources with appropriate knowledge and skills to perform ongoing activities.
- Create, manage, and control work plans, project schedules, and/or WBS
- Maintain quality control through repeatable, managed processes
- Change control management
- Documentation Management, including ensuring that information is stored in the appropriate ACF document repositories and configuration management tools
- Communications Management

- Risk Management including working with COR on timely escalation and resolution of risks
- Issue Management including working with COR on timely escalation and resolution of issues
- Quality Assurance
- Responding to general inquiries from ACF/OCIO staff overseeing program activities
- Coordinating with Government staff to ensure that tasks and their subtasks are executed in line with program direction, priorities, and processes
- Participate in meetings in different capacities, as required
- Prepare and track meeting agendas, minutes, issues, risks, and action items
- Create all required status reports and participate in progress reviews
- Track and manage cost expenditures
- Respond to ad hoc data calls
- Track monthly and cumulative performance metrics as applicable

The Contractor's Quality Control Plan (QCP) shall set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the Task Order. The Contractor's QCP shall set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the SOW.

In reference to the reporting activities, the COR will monitor performance and review reports, furnished by the Contractor to determine how the Contractor is performing. The Contractor shall be responsible for making required changes in processes and practices to ensure performance is managed effectively.

Coordination and Process Compliance

The Contractor shall ensure activities corresponding to tasks and their subtasks are coordinated effectively and conducted according to the established ACF/OCIO processes. Activities include, but are not limited to:

- Ensuring the participation of staff with relevant, complete, and current information at governance meetings, including the system workgroup meetings and customer status meetings
- As requested, ensuring participation of technical staff in working sessions with OCIO and program support contractor (s), continuous enhancement planning, support for program risk management, and compliance with Program Quality Assurance (QA) and Change and Release Management (CRM) procedures
- Identifying need for operations teams and end user communication resulting from Security and Privacy changes or updates
- Ensuring coordination between all the tasks and subtasks of this SOW

- Ensuring staff is familiar with and adhere to OCIO processes
- Identifying the changes impacting cross system or Task areas, dependencies and risks throughout the SDLC process, and ensuring the related activities are documented and coordinated
- Coordinating cross systems or cross teams for escalations and resolutions of complex security and privacy issues

In the event performance is not corrected the first time, the contractor must provide a Corrective Action Plan (CAP). Once approved, the Contractor shall execute the plan. If performance does not improve then the government moves to not paying for performance or termination.

Program Management Meetings

In addition to the Kick-Off meeting required in the Transition-In section of the SOW, the Contractor shall participate in meetings as directed by the ACF COR. The Contractor shall prepare and track meeting agendas, minutes, notes, issues, and action items. The Contractor shall prepare and provide the ACF COR with the meeting minutes of all status meetings. The Contractor shall prepare and provide other meetings minutes related to this Task Order as directed by the ACF COR or designated representative. Minutes shall be of sufficient detail to accurately document meeting data and location, meeting purpose, items discussed, decisions made, attendees, and action items. Meeting minutes shall be delivered within three business days following the meeting to parties as directed by the ACF COR or designated representative.

Task Order Reporting

Weekly Task Order Status Report

The Contractor shall submit a weekly status report, including the following types of information for each task and subtask defined in the Task Order:

- Activities and Accomplishments
- Deliverables
- Milestones
- Issues, Risks, and Mitigation Plans
- Planned Activities for the following reporting week
- Routine Monitoring Activities

The Contractor shall abide by a template or format agreed to or supplied by the ACF COR or designee. The Contractor shall abide by the due date agreed to or supplied by the ACF COR or designee.

Monthly Task Order Status Report

The Contractor shall submit a monthly status report, including the following types of information for each task and subtask defined on the Task Order:

- Activities and Accomplishments
- Deliverables
- Milestones
- Issues, Risks, and Mitigation Plans
- Planned Activities for following reporting period
- Routine Monitoring Activities

The Contractor shall abide by a template or format agreed to or supplied by the ACF COR or designee. The Contractor shall abide by the due date agreed to or supplied by the ACF COR or designee.

Contract Status and Performance Measures

The Contractor shall ensure that status and performance data is documented and tracked in a Performance Metrics Report (PMR). The Contractor shall establish their initial set of metrics and measures (the baseline) that will be used to monitor and control the Contractor's task execution. The Contractor's metrics should include the Government's minimum metrics, identified below, plus any additional ones it feels are needed to properly gauge the performance of the Contractor's activities.

Activity Supported	Metric
Management Plans (Objective: 95%, Threshold: 90%)	Compare issue resolution dates versus estimated date Compare risk resolution dates versus estimated date Compare progress versus schedule for activities scheduled
Progress Reports (Objective: 97%, Threshold: 90%)	Compare actual spending versus plan/limit, show variance Track monthly ratings
Deliverables (Objective: 97%, Threshold: 95%)	Compare completion dates versus scheduled dates Track number of revisions after scheduled submission Track rejected deliverables
Staffing (Objective: 100%, Threshold: 97%)	Compare staff versus key personnel Compare staff versus "required" personnel Track status of staff badging
Security (Objective: 100%, Threshold: 97%)	Compare clearances against security requirements Track security incidents
GFE	Check Asset Inventory versus Delivered GFE

(Objective: 100%, Threshold: 99%)	
Travel (Objective: 97%, Threshold: 90%)	Track authorizations Compare actual spending versus plan/limit
ODC (Objective: 97%, Threshold: 90%)	Track actual ODC versus plan/limit Track authorizations
Operations (Objective: 99%, Threshold: 90%)	Track System uptime Track planned change duration versus actual duration

Table 1

Monthly Task Order Financial Reports

The Contractor shall create and provide a Monthly Task Order Financial Report that contains line items for each task, subtask, and project and display labor category, rate, planned and actual hours worked, and other charges incurred for each resource.

The Contractor shall abide by a template or format agreed to or supplied by the ACF COR or designee. The Contractor shall abide by the due date agreed to or supplied by the ACF COR or designee. The details and format required for this report may be adjusted at any time by ACF COR or designee.

Support for Capital Planning and Investment Control

The ACF OCIO is required to manage and produce reports to HHS and other federal agencies. The Contractor shall respond to ACF OCIO's data calls, requests for input and ad hoc support necessary for ACF OCIO to comply with Capital Planning and Investment Control (CPIC), OMB Circular A-11 requirements for ACF systems, enterprise architecture and strategic planning which occur in differing reporting cycles.

The Contractor shall support and provide data required by ACF OCIO to manage the ACF Investment Portfolio and develop operating procedures for presentation to the governance boards in accordance with the standards required by the Clinger-Cohen Act.

7. Development, Modernization, and Enhancement

DEVELOPMENT, MODERNIZATION AND ENHANCEMENT

The purpose of this task is to provide development, modernization and enhancement to OPS. This will also include new development and COTS implementations. The modernization efforts will include infusion of newer technologies in the areas including but not limited to data management, data warehouse, business intelligence and data quality, analytical tools, web services and support for handheld/mobile devices. Development, Modernization and Enhancement to be provided may vary from one service area to another. Examples of service areas may include:

- Requirement Analysis
- Design and Development
- Testing
- Implementation

Subtask 1- Requirement Analysis

The Contractor shall perform requirements analysis, as tasked. Representative activities include, but are not limited to:

- Analyze, decompose and translate the requirements into detailed functional and non-functional system requirements
- Work with the project team, including user representatives, to review and validate the system requirements
- Develop the System Requirements Specifications (SRS)
- Create/Update Concept of Operations (ConOps)
- Establish a finalized Requirements Traceability Matrix (RTM)
- Complete a successful requirements analysis stage gate review including coordination of review meeting, preparation of materials, and resolution of any issues identified by critical partners

Subtask 2- Enhancement Design and Development

The Contractor shall perform design and development activities, as tasked. Representative tasks include, but are not limited to:

- Design software enhancements based on the detail requirements identified, verified, documented and approved in the requirements analysis phase
- Develop/update the System Design Document (SDD)
- Create/Update Interface Control Document(s) to be used when interfacing with exiting reporting systems
- Test the design against the Requirements Traceability Matrix
- Develop Test artifacts: Master/Release Test Plan, Test Case Specifications
- Work with the COR and project team in the verification and approval of the design at designated milestones and update Project artifacts accordingly
- Develop/update all application/system code required to build the system according to the System Design Document
- Construct/Update Software Application Modules
- Develop all application/system code in compliance with 508 requirements, ACF defined IT standards and approved software on ACF approved hardware.
- Use an iterative development approach supporting prototypes and demos throughout the development process

- Develop system/application code level documentation with particular emphasis on source code documentation
- Conduct and document unit testing
- Track and correct all defects before completion of development phase
- Complete a successful design & development stage gate review including coordination of review meeting, preparation of materials, and resolution of any issues identified by critical partners

Subtask 3 - Testing

The Contractor shall review and test the new solution to ensure that all links (new and changed features links) are functioning, and that the solution is in compliance with the project requirements. As tasked, the Contractor shall perform Test and Evaluation Services to support all testing and evaluation phase requirements of the SDLC and as determined by ACF. Any issues identified as a result of this initial testing shall be reported to the COR and Project Manager and corrected by the Contractor.

Acceptance Testing

The Contractor shall be responsible for the support and coordination of User Acceptance Testing (UAT) activities. After training, the COR and Project Manager and the Contractor will select a set of tests to evaluate all functions, templates and options. Selected testers shall intentionally stress the system to identify weaknesses which will be reported to the Contractor for resolution.

These initial tests will not be visible to the public through this testing phase although it will be operating in the pre-production environment. Any issues identified during this process shall be addressed and resolved by the Contractor.

The UAT Test Results Report is provided to the project manager and senior project stakeholders and summarizes the UAT results and whether the UAT objectives were met. It covers:

- Achievement of UAT objectives
- Test execution results by test cycle
- Test execution statistics and trends
- A plan to address any UAT test issues still unresolved

Subtask 4 - Implementation

The Contractor shall provide full Implementation services end to end support during all phases of the implementation process with skilled resources. The Contractor shall employ a professional, implementation, and integration framework approach. The formal approach to quality assurance through the use of quality system standards such as Capability Maturity Model Integration (CMMI) level 2 or higher, ISO 9001-2001, SSAE-16 standards are required. All efforts shall support implementation/integration of system and other software.

The Contractor shall provide documentation, setup, test plans, solution demonstration, knowledge transfer sessions, conversion, and reconciliation support.

Implementation shall be conducted through a phased approach. The Contractor will work to ensure the new solution is properly installed and configured. The Contractor shall provide implementation/integration services using ACF CCB approved products and services where applicable.

Security Requirements for Development or Enhancement of a Federal IT System

1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC or ACF SDLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012) or current ACF frameworks and policies.

2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

3)The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.

4) The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

5) The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data shall be used during software testing.

6) The Contractor (and/or any subcontractor) shall protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

Requirements for New Websites and Digital Services and Redesigns of an Existing Legacy Website or Digital Service

An executive agency that creates a website or digital service that is intended for use by the public, or conducts a redesign of an existing legacy website or digital service that is intended for use by the public, shall ensure to the greatest extent practicable that any new or redesigned website, web-based form, web-based application, or digital service—

1) is accessible to individuals with disabilities in accordance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d);

2) has a consistent appearance;

3) does not overlap with or duplicate any legacy websites and, if applicable, ensure that legacy websites are regularly reviewed, eliminated, and consolidated;

4) contains a search function that allows users to easily search content intended for public use;

5) is provided through an industry standard secure connection;

6) is designed around user needs with data-driven analysis influencing management and development decisions, using qualitative and quantitative data to determine user goals, needs, and behaviors, and continually test the website, web-based form, web-based application, or digital service to ensure that user needs are addressed;

7) provides users of the new or redesigned website, web-based form, web-based application, or digital service with the option for a more customized digital experience that allows users to complete digital transactions in an efficient and accurate manner; and

8) is fully functional and usable on common mobile devices.

8. Contract Transition Management

CONTRACT TRANSITION MANAGEMENT

Transition-Out Plan

The Contractor shall develop and submit a transition plan within 90 days prior to the expiration of the contract award. The Contractor's transition plan shall be approved by ACF OCIO and shall contain a milestone schedule of events and system turnovers. The Contractor shall transition systems with no disruption in operational services.

The contractor shall plan and participate in weekly meetings between the COR and other participants as identified by ACF OCIO. The meetings will be held at the ACF Switzer Building at 330 D Street, Washington, D.C. location.

The Contractor shall prepare and submit an agenda two (2) business days prior to each meeting and prepare and provide meeting minutes within 24 hours after the meeting. The meeting minutes, at a minimum, shall include the following:

1. List of participants
2. Purpose of the meeting
3. Decisions reached during the meeting
4. Action items identified (including the person responsible for addressing the action and the date the action is to be completed)

5. Date, time, and location of next meeting

Deliverable(s): Transition Plan, Meeting Agendas, Meeting Minutes

TRANSITION FROM AN EXISTING CONTRACTOR TO INCOMING CONTRACTOR/GOVERNMENT PERSONNEL

Transition Out

No less than 90 days prior to the end of this contract, the contractor shall provide transition services / phase-out support to ACF/OCIO. During this transition period, the contractor shall work with the ACF/OCIO Government personnel, as well as other identified ACF/OCIO Contractors. The contractor shall coordinate with the new contractor and/or Government personnel to transfer knowledge on the following technical documentation, including leasing, licenses, project management and knowledge bases.

The Contractor shall provide:

- Current versions of all CONOPS, operational procedures, standard operating procedures, guidelines, performance reports, specifications for hardware and software, and other pertinent information needed to continue the services being performed by the Contractor;
- “Shadowing” and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by the Contractor;
- Full source code sets (not COTS source code) with configuration management information;
- Identification of actions required of the Government in sufficient time to assure seamless transition;
- A milestone chart detailing the timelines and stages of transition from the effective date of performance of the successor until the successor assumes sole responsibility for the work;
- Points of Contacts;
- Provide Government Information/Equipment/Property along with full support in the reconciliation of this inventory;
- Status of technical initiatives;
- A communication plan and a training plan for handing over information and responsibilities in a seamless manner to the ACF/OCIO Government personnel;
- Transition of Key Personnel;
- Identification of the individuals (at all levels) who are responsible for the transition and their respective roles, detailed lines of communication, and how the incumbent Contractor will interface with ACF/OCIO during this phase of contract performance.
- Lessons learned

Deliverable(s): Inventory of GFI/GFE/GFP, O&M Manual, User Manual, All System Documentation, System Design Document, Release Plan, Interface Design Document, Data Use Agreement, Test Case Specification, Test Summary Report, User Acceptance Testing, Training Plan, Training Materials, Implementation Plan, Test Reports, Communication Plan, Project Completion Report, Annual Operational Analysis, Disposition Plan, Project Archives

TRANSITION PLANS AND PROCEDURES

The contractor shall work collaboratively with government personnel identified by ACF/OCIO to ensure a seamless transition of the activities included in this SOW and the respective task order and/or contract award. The contractor shall provide:

- A transition milestones and timeframes, including a detailed timeline for work-in-progress;
- A comprehensive listing of the responsibilities of all personnel participating in the transition to include the policies, practices, and procedures to be employed by the incumbent contractor to ensure there is no conflict between routine program maintenance and the activities of the transition;
- An in-depth schedule and thorough description of the methodology employed by the incumbent contractor to ensure no degradation of service during the transition period;
- A risk management plan that includes a list of the potential risks during the transition period and the plan to mitigate each;
- A complete and detailed resource-planning/resource-turnover analysis; and
- Any travel necessary to support the transition.

Deliverable(s): Timeline and Milestone; list of personnel, policies, practices and procedures, schedule and description of methodology, risk management plan, resource-planning/resource turnover analysis, travel cost

9. Records Management (Include in Section H.)

RECORDS MANAGEMENT OBLIGATIONS

A. *Applicability*

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes ACF records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their ACF contract.
4. may include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

   Electronic information system means an information system that contains and provides access to computerized Federal records and other information. (36 CFR 1236.2)

   The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself. (36 CFR 1236.10)

   (a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

   (b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

   (c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

   (d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.

(g) Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. ACF and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of ACF or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report it to ACF immediately. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to ACF control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts.

The Contractor (and any sub-contractor) is required to abide by Government and HHS and ACF guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with HHS and ACF policy.
8. The Contractor shall not create or maintain any records containing any non-public HHS or ACF information that are not specifically tied to or authorized by the contract.
9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
10. ACF owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which ACF shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take ACF-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. *Flowdown of requirements to subcontractors*

1. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract, and require written subcontractor acknowledgment of same.
2. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

10. QASP

Quality Assurance Surveillance Plan (QASP)

The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the contract and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance and provides verifiable input for the Contractor Performance Assessment Reporting System (CPARS). The QASP may be updated by modification to the contract. The QASP shall provide the basis for performing and controlling the project's activities in accordance with the Contract.

11. HHS Section 508 Accessibility Standards

The following Section 508 accessibility standards apply to the work to be performed

A. Section 508 of the Rehabilitation Act of 1973

In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. The law (29 U.S.C § 794 (d)) applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508, agencies must give disabled employees and members of the public access to information comparable to the access available to others.

The U.S. Access Board is responsible for developing Information and Communication Technology (ICT) accessibility standards to incorporate into regulations that govern Federal procurement practices. On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508, and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018.

The rule updated and reorganized the Section 508 Standards and Section 255 Guidelines in response to market trends and innovations in technology. The refresh also harmonized these requirements with other guidelines and standards both in the U.S. and abroad, including standards issued by the European Commission, and with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG 2.0), a globally recognized voluntary consensus standard for web content and ICT.

https://www.section508.gov/manage/laws-and-policies

The Architectural and Transportation Barriers Compliance Board (Access Board issued final guidelines for accessibility, usability, and compatibility of telecommunications equipment and customer premises equipment covered by section 255 of the Telecommunications Act of 1996. Section 255 of the Communications Act, as amended by the Telecommunications Act of 1996, requires telecommunications products and services to be accessible to people with disabilities. Manufacturers must ensure that products are “designed, developed, and fabricated to be accessible to and usable by individuals with disabilities” when it is readily achievable to do so. Accessibility guidelines issued by the Board under Section 255 address the telecommunications products covered including:

- wired and wireless telecommunication devices, such as telephones (including pay phones and cellular phones), pagers, and fax machines
- other products that have a telecommunication service capability, such as computers with modems
- Equipment that carriers use to provide services, such as a phone company’s switching equipment.

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-telecommunications-act-guidelines

Subpart C -- Functional Performance Criteria

Section 1194.31 Functional Performance Criteria

This section provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific requirement under other sections. These criteria are also intended to ensure that the individual accessible components work together to create an accessible product. This section requires that all product functions, including operation and information retrieval, be operable through at least one mode addressed in each of the paragraphs. Go to Sub-part C Functional Performance Criteria 1194.31 at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards#subpart_c

FAR -- Part 39

Acquisition of Information Technology

39.000 -- Scope of Part.

(FAC 2005-82)

11.1.1. 39.000 -- Scope of Part.

This part prescribes acquisition policies and procedures for use in acquiring—

(a) Information technology, including financial management systems, consistent with other parts of this regulation, OMB Circular No. A-127, Financial Management Systems and OMB Circular No. A-130, Management of Federal Information Resources; and

(b) Information and information technology.

11.1.2. 39.001 -- Applicability.

This part applies to the acquisition of information technology by or for the use of agencies except for acquisitions of information technology for national security systems.

11.1.3. 39.002 -- Definitions.

As used in this part--

“Modular contracting” means use of one or more contracts to acquire information technology systems in successive, interoperable increments.

B. Subpart 39.1 – General

11.1.4. 39.104 – Information Technology Services.

When acquiring information technology services, solicitations must not describe any minimum experience or educational requirement for proposed contractor personnel unless the contracting officer determines that the needs of the agency—

(a) Cannot be met without that requirement; or

(b) Require the use of other than a performance-based acquisition (see Subpart 37.6).

11.1.5. 39.106 -- Contract Clause.

The contracting officer shall insert a clause substantially the same as the clause at 52.239-1, Privacy or Security Safeguards, in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.

C. Subpart 39.2 – Electronic and Information Technology

11.1.6. 39.201 Scope of subpart.

(a) This subpart implements section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

(b) Further information on section 508 is available via the Internet at http://www.section508.gov.

(c) When acquiring EIT, agencies must ensure that--

(1) Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities; and

(2) Members of the public with disabilities seeking information or services from an agency have access to and use of information and data that is comparable to the access to and use of information and data by members of the public who are not individuals with disabilities.

11.1.7. 39.202 Definition.

Undue burden, as used in this subpart, means a significant difficulty or expense.

11.1.8. 39.203 Applicability.

(a) Unless an exception at 39.204 applies, acquisitions of EIT supplies and services must meet the applicable accessibility standards at 36 CFR part 1194.

(b)

(1) Exception determinations are required prior to contract award, except for indefinite-quantity contracts (see paragraph (b)(2) of this section).

(2) Exception determinations are not required prior to award of indefinite-quantity contracts, except for requirements that are to be satisfied by initial award. Contracting offices that award indefinite-quantity contracts must indicate to requiring and ordering activities which supplies and services the contractor indicates as compliant and show where full details of compliance can be found (*e.g.,* vendor's or other exact website location).

(3) Requiring and ordering activities must ensure supplies or services meet the applicable accessibility standards at 36 CFR part 1194, unless an exception applies, at the time of issuance of task or delivery orders. Accordingly, indefinite-quantity contracts may include

noncompliant items; however, any task or delivery order issued for noncompliant items must meet an applicable exception.

(c)

(1) When acquiring commercial items, an agency must comply with those accessibility standards that can be met with supplies or services that are available in the commercial marketplace in time to meet the agency's delivery requirements.

(2) The requiring official must document in writing the no availability, including a description of market research performed and which standards cannot be met, and provide documentation to the contracting officer for inclusion in the contract file.

11.1.9. 39.204 Exceptions.

The requirements in 39.203 do not apply to EIT that--

(a) Is purchased in accordance with Subpart 13.2 (micro-purchases) prior to April 1, 2005. However, for micro-purchases, contracting officers and other individuals designated in accordance with 1.603-3 are strongly encouraged to comply with the applicable accessibility standards to the maximum extent practicable;

(b) Is for a national security system;

(c) Is acquired by a contractor incidental to a contract;

(d) Is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment; or

(e) Would impose an undue burden on the agency.

(1) *Basis*. In determining whether compliance with all or part of the applicable accessibility standards in 36 CFR part 1194 would be an undue burden, an agency must consider--

(i) The difficulty or expense of compliance; and

(ii) Agency resources available to its program or component for which the supply or service is being acquired.

(2) *Documentation.*

(i) The requiring official must document in writing the basis for an undue burden decision and provide the documentation to the contracting officer for inclusion in the contract file.

(ii) When acquiring commercial items, an undue burden determination is not required to address individual standards that cannot be met with supplies or service available in the commercial marketplace in time to meet the agency delivery requirements (see 39.203(c)(2) regarding documentation of nonavailability). http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm

Provisions and Clauses:

When purchasing consulting services and labor hours to provide development, authoring, testing, installation, configuration, maintenance, training, and other consulting services related to ICT.

The Contractors shall ensure the personnel providing the labor hours possess the knowledge, skills, and ability necessary to address the applicable Revised 508 Standards defined in this contract and shall provide supporting documentation upon request.

When the Contractors provides custom ICT development services pursuant to this contract, the Contractors shall ensure the ICT fully conforms to the applicable Revised 508 Standards prior to delivery and before final acceptance.

Installation, Configuration & Integration Services

When the Contractors provides installation, configuration or integration services for equipment and software pursuant to this contract, the Contractors shall not install, configure or integrate the equipment and software in a way that reduces the level of conformance with the applicable Revised 508 Standards.

The Contractors shall ensure maintenance upgrades, substitutions, and replacements to equipment and software pursuant to this contract do not reduce the original level of conformance with the applicable Revised 508 Standards at the time of contract award.

The contractor shall test and validate the ICT solution for conformance to the Revised 508 Standards, in accordance with the agency required testing methods.

- Contractors shall validate conformance to the applicable Revised 508 Standards using a defined testing process. The Contractors must describe test process and provide the testing results to the agency. The testing shall include type of Assistive Technology (AT) and automatic tools used for validating testing.

The Contractors shall maintain and retain full documentation of the measures taken to ensure compliance with the applicable requirements, including records of any testing or demonstrations conducted. Before acceptance, the contractor shall provide an **Accessibility Conformance Report (ACR)** for each ICT item that is developed, updated, configured for the agency, and when product substitutions are offered. The ACR should be based on the latest version of the Voluntary Product Accessibility Template (VPAT)).

To be considered for award, an ACR must be submitted for each ICT Item, and must be completed according to the instructions provided by ITIC.

Before acceptance, when the contractor is required to perform testing to validate conformance to the agency's accessibility requirements, the vendor shall provide a **Supplemental Accessibility Conformance Report (SAR)** that contains the following information:

- Accessibility test results based on the required test methods.
- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation on how to configure and install the ICT item to support accessibility.
- When an ICT item is an authoring tool that generates content (including documents, reports, videos, multimedia productions, web content, etc.).

Before final acceptance of any ICT item, including updates and replacements, if the Contractors claims its products or services satisfy the applicable Revised 508 Standards specified in the statement of work, and the contracting officer determines that any furnished ICT item is not in compliance with such requirements, the contracting officer will promptly inform the Contractors in writing of the noncompliance. The Contractors shall, at no cost to the agency, repair or replace the non-compliant products or services within the period specified by the contracting officer.

Revised 508 Standards, Safe Harbor and FAR Update

Federal agencies have been working to transition to the Revised 508 Standards, which aim to make information technology more accessible to all users, and bring U.S. accessibility standards in line with international standards. The FAR Council is also working on regulatory updates to the Federal Acquisition Regulation (FAR), and as of January 18, 2018, agencies should proactively address the requirements of the Revised 508 Standards in their procurement processes. Note that all new or revised information and communication technology (ICT) must satisfy the Revised 508 Standards, but older ICT (previously referred to as Electronic and Information Technology (EIT)), providing that it was compliant with the Original 508 Standards, may fall under a "safe harbor" provision.

- **Safe Harbor** - The Revised 508 Standards also include a "safe harbor" provision for existing (i.e., legacy) ICT. Under this safe harbor, unaltered, **existing ICT (including electronic content) that complies with the Original 508 Standards need not be modified or upgraded to conform to the Revised 508 Standards.**
    - This safe harbor applies on an element-by-element basis to each component or portion of the existing ICT, with each component or portion assessed separately.
        - **Existing, unaltered ICT that did not comply with the Original 508 Standards as of January 18, 2018 must now be brought into compliance with the Revised 508 Standards. Please visit https://www.section508.gov/blog/Revised-508-Standards-Safe-Harbor-and-FAR-Update**

[2] According to the Section 508 standards, part 1194.2, "(b) When procuring a product, agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards."

Contract Staff and Vendors
Misrepresentation of Section 508 compliance or failure to provide ICT products or services that meet the proposed and accepted level of conformance is unacceptable. They may result in termination for cause or other actions as specified in the HHSAR or FAR.

(a) In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offeror must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offeror or developers to self-evaluate their supplies and document—in detail—

whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy. (See HHS PAT Link below.

To determine whether proposed EIT services meet applicable Section 508 accessibility standards, offeror must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

(a) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS website: (http://www.hhs.gov/web/508). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
(b) The leaderboard below demonstrates how compliant our websites are with Section 508. The accessibility of websites for each Operating Division is determined each month by an automated scan of every page of every website.

Scores
Acceptable- 76% and above
Needs Improvement- 75.99% and below

Deliverable (s): Schedule for Contractor Submission of Section 508 Annual Report, Annually at the start of each option.

In addition to Section 508 requirements, HHS has policies, standards, and requirements for electronic documents that include but aren't limited to the following:

- Document file name should not contain any spaces or special characters.
- Document file name needs to be concise, generally limited to 20-30 characters and should clarify the contents of the file.
- All Document properties should be filled out Title, Author, (an HHS OpDiv, StaffDiv, or Program Office---not an individual's names) Subject, and Keywords
- Use electronic version for any signatures (see http://webstandards.hhs.gov/standards/41)
- Use Exit Icon disclaimer for all non-government sites

12. List of Deliverables (To be added based on tasks included in SOW)

Deliverable Name	Deliverable Title/Description	Due Date
Roster	Roster of all employees	Within 3 days of the effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)	Assist in the completion of a PTA/PIA form	Within 30 days after the contract award
Training Records	Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Rules of Behavior	Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Response Report	Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident Response Plan	Incident and Breach Response Plan	Upon request from government
Personnel Security Responsibilities (onboarding)	List of Personnel with defined roles and responsibilities	Within 3 days that is before an employee begins working on this contract.
Personnel Security Responsibilities (off-boarding)	Off-boarding documentation, equipment and badge when leaving contract	Within 3 days after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.
Background Investigation Documentation	Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS/ACF
Certification of Sanitization of Government and Government Activity-	Form or deliverables required by ACF.	At contract expiration.

Related Files, Information, and Devices.		
Contract Initiation and Expiration	If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration.
Security Assessment and Authorization (SA&A)	SA&A Package • SSP • SAR • POA&M • Authorization Letter • CP and CPT Report • E-Auth (if applicable) • PTA/PIA (if applicable) • Interconnection/Data Use Agreements (if applicable) • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other ACF-specific documents	Due date to be determined and approved by ACF OCIO based on planned deployment and ATO schedule
Reporting and Continuous Monitoring	Revised security documentation/Agreements	As required by ACF OCIO
Security Alerts, Advisories, and Directives	List of personnel with designated roles and responsibilities	As required by ACF OCIO
Incident Reporting	• Incident Reports (as needed) • Incident Response Plan	Incident Response plan provided in accordance with ATO schedule and yearly thereafter (Prior to production deployment or go live date) Incident Reports provided quarterly and upon request
Other IT Procurements (Non-Commercial and Open Source	• Computer Software, including the source code	Prior to performing any work on behalf of HHS

Computer Software Procurements)		