**SECTION B. SUPPLIES OR SERVICES AND PRICES/ COST**

# B.1 GENERAL

The work shall be performed in accordance with all Sections of this Call Order and the contractor’s Parent PSC BPA 75P00119A00091, under which the resulting Call Order is being placed.

**B.2 TYPE OF CONTRACT**

The contractor shall perform the effort required by this Call Order on a Firm Fixed Price basis.

# B.3 SERVICES AND PRICE

The following abbreviation are used tin the price schedule:

|  |  |
| --- | --- |
| IAW | In Accordance With |
| CLIN | Contract Line Item Number |
| FFP | Firm-Fixed Price |
| NTE | Not-to-Exceed |
| QTY | Quantity |

In consideration for successful performance of this work, the contractor shall be compensated for the completion of the following tasks:

|  |
| --- |
| ***DESCRIPTION*** |
| Set-up and Implement SWIFT Mail Digitization – IAW Task 1 |
| Develop, Deploy, and Implement SWIFT Digital Mail Stop Delivery – IAW Task 2 |
| Develop, Deploy, and Implement SWFIT Accountable Mail – IAW Optional Task 3 |

**B.3.1 ORDERING PERIOD:**

**Period of Performance – 08/1/2023 to 07/31/2024**

# FFP Labor CLINs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CLIN** | **Description** | **QTY** | **Unit** | **Total NTE**  **Ceiling** |
| **001** | SWIFT Digital Mail Enhancements  (Tasks 1 and 2) | 1 |  | $695,000.00 |
| **002** | Optional SWIFT Accountable Mail Enhancements (Task 3) | 1 |  | $70,000.00 |

# B.4 WORK HOURS/ HOLIDAYS

Work may occur only Monday – Friday, excluding all federal holidays, between 7:00AM – 5:30PM. No services or deliveries shall be performed on Saturdays, Sundays or Federal legal holidays. Deliverables due on a Saturday, Sunday, or Federal holiday shall be due on the following business day.

# OBSERVANCE OF FEDERAL HOLIDAYS

New Year’s Day January 1st

Martin Luther King’s Birthday Third Monday in Jan.

President’s Day Third Monday in Feb.

Memorial Day Last Monday in May

|  |  |
| --- | --- |
| Juneteenth  Independence Day | June 19th July 4th |
| Labor Day | First Monday in Sept. |
| Columbus Day | Second Monday in Oct. |
| Veteran’s Day | November 11th |
| Thanksgiving Day | Fourth Thursday Nov. |
| Christmas Day | December 25th |

**SECTION C. DESCRIPTION/ SPECIFICATIONS/ PERFORMANCE WORK STATEMENT**

# C.1 SCOPE AND BACKGROUND

**Purpose**

This task is to acquire IT services for the ACF Executive Secretary in support and enhancements of correspondence control with the Strategic Work Information and Folder Transfer (SWIFT).

**Background**

SWIFT is a mission critical application that ACF continues to rely on to route and track correspondences within HHS and ACF. SWIFT currently resides at the Government Transformation Center (application hosting facility) in Reston Virginia.

As a result of office closures and a shift to remote workforce, ACF would like to transition from delivery of physical mail to digital mail using the ACF SWIFT system. ACF would like to model its digital transition after the SWIFT digital mail experience currently in use by other HHS Agencies. Building on this experience, ACF requested services designed to accomplish the following overarching requirements:

* Support the digitization of physical mail delivered to a central location
* Build a solution in SWIFT to support the digital routing and delivery of mail to digital mail stops
* Train scanning operators in the use of digitization of mail
* Implement and train ACF digital mail recipients
* Support the ongoing maintenance and operations of the new SWIFT ACF digital mail solution

**Goal and Objectives**

The objective of this Statement of Work (SOW) is to obtain IT services to enhance the SWIFT system, from Sole Solutions Inc. in support of the Digitization of ACF Mail. These services will be procured using the existing SSI SWIFT BPA contract (ID 75P00119A00091), under Task 3 of the BPA titled *Application Design, Development, Test and Deployment*.

# C.2 TASKS

## C.2.1 TASK 1- Set-up and Implement SWIFT Mail Digitization

The establishment of SWIFT digital mail intake requires proper planning and technical support. Paper mail correspondence is delivered by PSC to the ACF Mary E. Switzer building. Once this letter correspondence is delivered, it needs to be scanned and routed to the ACF SWIFT system. To set-up this workflow and technical process, the Contractor must coordinate with ACF to evaluate and acquire the necessary hardware for scanning and sending documents to SWIFT. The hardware must be configurable to integrate with SWIFT and of high-quality, production-level quality. The Contractor shall work with ACF to plan the space for proper intake operations, install and test the scan drivers, and calibrate the hardware for optimal image capture and transfer to SWIFT.

The Contractor shall configure a software solution for batch mail utilizing Kodak Alaris Capture Pro software. Barcoded separator sheets and batch configuration options will permit ACF personnel to easily stack letters for efficient scanning intake operations. The intake process is configured to OCR the digitized envelope and capture addresses for automated data entry (quality dependent feature). The SWIFT solution shall ensure that each letter is processed by OCR and a PDF is produced that displays the letter image with background selectable text. The SWIFT software solution shall be integrated to enhance the accessibility of the PDF by applying the required tags to document structures for improved screen reader navigation.

The Contractor shall integrate Alaris Capture Pro with a new SWIFT Digital Mail application module for seamless delivery to ACF mail stops (i.e., SWIFT Gatekeeper Boxes). The Contractor shall configure SWIFT so that manual data entry or application switching is not required by users. Mail correspondence shall be routed through the SWIFT Digital Mail application automatically when the batch is saved by the scan operator.

Scan intake operators shall be trained based upon the SWIFT Digital Mail business processes developed by the Contractor in coordination with ACF. Supported business processes shall include initial paper correspondence capture, initial quality assurance, and the following SWIFT requests: paper delivery, rescan, reassignment, and paper destruction in accordance with ACF records management policy.

## C.2.2 TAKS 2- Develop, Deploy, and Implement SWIFT Digital Mail Stop Delivery

SWIFT shall be configured to support routing of mail correspondence at two levels. Task 1 addresses routing to SWIFT mail stops or Gatekeeper Boxes within the organization. Task 2 addresses routing by mail stop users to the final individual recipient or group within the organization.

Monitoring, sorting and re-delivering letters that arrive at an ACF mail stop is rarely a person’s full-time role in the organization. The SWIFT digital mail stop solution must provide ample notification of incoming mail, an intuitive method of re-delivery, and visibility on unread mail that may require further action.

**Implementing a Digital Mail Stop Application** – The Contractor shall configure a digital mail stop solution utilizing the SWIFT platform. SWIFT provides a proven platform at ACF with secure, transparent single sign and workflows that reach every member of the organization. No user-based licensing requirements make the platform ideal for wide-reaching business line applications such as enterprise digital mail.

The SWIFT digital mail stop solution shall provide notifications of incoming mail, an “inbox” for incoming mail, user customized “delivery zones” for easy drag & drop delivery, and functionality to deal with exceptions such as rescan requests, paper delivery requests and returns for reassignment.

I**ntegration with Existing Systems** – Today the ACF Executive Secretariate receives mail addressed to the ACF Leadership in paper format and relies upon desktop scanners to upload into the SWIFT Correspondence Module. As part of this task, the Contractor shall integrate the new SWIFT Digital Mail application with the existing SWIFT Executive Correspondence application. Exec Sec personnel will no longer be required to scan important mail on low-end desktop scanners. Mail will be digitized with other ACF mail in a central location. This will be done on high-end hardware, generating high quality, accessible images. Digitized letters will seamlessly flow into the Exec Sec where users can perform their SWIFT functions efficiently and remotely. The ACF SWIFT Digital Mail application will be developed in a way that supports integration of other business applications.

**SWIFT Configuration** – The Contractor shall use a Systems Development Life Cycle (SDLC) framework, which is fully compliant with the HHS EPLC processes. SDLC provides a standard sequence of activities for requirements analysis, design, and solution configuration. The Contractor shall configure and test the SWIFT application to support digital mail. The Contractor shall migrate the application modules from the development environment to the test environment. Once the Contractor has completed the system configuration and regression testing, the Contractor shall prepare installation scripts and packages, and migrate the modules to the SSI quality assurance environment in a mock deployment exercise to test the deployment procedure and integrity of the installation package.

Throughout the process the Contractor shall participate in ACF stage gate meetings to review system requirements, design, test plans and final readiness. At each stage gate meeting, the Contractor shall present required project artifacts and give a brief detailed presentation describing the current phase of the project. In addition, the Contractor shall meet regularly with an Integrated Project Team (IPT) consisting of participating stakeholders and contractors.

At least two weeks prior to the scheduled release date, the Contractor shall deploy the solution to the ACF test environment where the customer has a final opportunity to review the new features during user acceptance testing. The Contractor shall conduct pre-deployment testing on any changes to the production baseline and will obtain zero production defects as part of regression testing.

Upon approval, the Contractor shall release the updated application and configuration to the ACF Production environment. Any necessary production data conversion or data migration to the updated environment shall also occur at this time. The Contractor shall provide updates to existing user documentation and release notes with any application update.

A key part of implementation is communicating with and training SWIFT application users. The Contractor shall work to draft and support the distribution of communications necessary to transition users to the new SWIFT Digital Mail application. Communication shall include updates on when training will occur, system go-live, and other relevant release updates. Training materials shall be created to offer users instructional references and hands-on experience. Users shall be trained in a group training series, with the opportunity for follow-up Q&A and one-on-one instruction as needed to reinforce initial learning concepts. These efforts are designed to promote strong user adoption and efficient usage of the new Digital Mail application. Once the system is live, users shall be supported through a Contractor staffed Help Desk, which must be customized to provide technical assistance specific to the ACF Digital Mail application.

## C.2.3 OPTIONAL TASK 3 – Develop, Deploy, and Implement SWIFT Accountable Mail

A portion of the mail received by ACF from external carriers (e.g. FedEx, USPS, UPS) requires a signature to confirm delivery. This type of mail is referred to as Certified or Accountable Mail and requires ACF personnel to collect physical mail from the Mail Center.

In conjunction with Task 2, the Contractor shall configure the SWIFT platform to include the capture and digital delivery of Accountable Mail that is scannable. Non-scannable Accountable mail will be physically delivered. SWIFT intake personnel and ACF users will be trained on the usage of the SWIFT Accountable Mail functionality.

# C.3 INFORMATION SECURITY AND/OR PHYSCAL ACCESS SECURITY REQUIREMENTS

All applicable and required procedures related to information security and/or physical access security requirements automatically flow down from the master BPA, to all supporting Call Orders.

# C.4 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.

# C.5 SECTION 508 ACCESSIBILITY STANDARDS

All applicable and required procedures related to section 508 accessibility standards automatically flow down from the master BPA, to all supporting Call Orders.

# SECTION D. MARKINGS

All applicable and required procedures related to packaging and marking automatically flow down from the master BPA, to all supporting Call Orders.

All deliverables required under this contract shall be packaged, marked and shipped in accordance with Government specifications. At a minimum, all deliverables shall be marked with the Call Oder number and Contractor name. The Contractor shall guarantee that all required materials shall be delivered in immediate usable and acceptable condition.

# D.1 MARKINGS

All reports and documentation required as deliverables in accordance individual Call Orders shall be marked as follows:

* Name of Contractor.
* Deliver Order Number DO/TO: 75P0011A00091/75ACF121F80047
* Title or description of the item(s) contained therein.
* Call Order COR’s name and address.

**SECTION E. ACCEPTANCE CRITERIA**

# E.1 INSPECTION AND ACCEPTANCE

Pursuant to FAR 52.212-4, Contract Terms and Conditions—Commercial Items, based on the selected contract type all work described within the contract are subject to final inspection and acceptance by an authorized representative of the Government.

All work under this contract is subject to inspection and final acceptance by the Contracting Officer or the duly authorized representative of the government.

The Government’s Contracting Officer’s Representative (COR) is a duly authorized representative of the government and is responsible for inspection and acceptance of all items to be delivered under this contract.

# E.1.1 ACCEPTANCE CRITERIA

Unless otherwise specified by the COR, the general quality measures, as set forth below, will be applied to each work product received from the Contractor under this contract.

Quality: Work products shall be accurate, and a system of quality control established that results in finished products that need little revision.

Design/Visual Value: Work products shall be accepted that meet standards and add to the value of the message through visual representation.

Consistency to Requirements: All work products must satisfy the requirements of this statement of work.

Timeliness: Work products shall be performed on a schedule commensurate with complexity and established need.

Technical Acumen: Techniques are used that produce good products; ways to improve are consistently sought through new methods of work and emerging technologies.

# E.1.2 APPROVALS BY THE COR

Pursuant to 52.212-4, *Contract Terms and Conditions—Commercial Items* all work delivered within this contract is subject to final inspection and acceptance by an authorized representative of the Government. The authorized representative of the Government is the Government's COR, who is responsible for inspection and acceptance of all services, materials, or supplies to be provided by the Contractor.

All services delivered to the COR will be deemed to have been accepted 30 calendar days after date of delivery, except as otherwise specified in this contract, if written approval or disapproval has not been given within such period. The COR’s approval or revision to the services delivered shall be within the general scope of work stated in this contract.

**SECTION F. DELIVERIES OR PERFORMANCE**

# F.1 PERIOD OF PERFORMANCE – Severable Services

The period of performance is a based period of 12 months. Any extension to the below period of performance shall be approved by the Contracting Office prior to the extension.

**Base Period:** September 30, 2023 through September 29, 2024

# F.2 PLACE OF PERFORMANCE

The majority of the work will be performed at the contractor facility and as required at the

Switzer building in Washington DC or Triple-I site in Reston if necessary. No Local

Washington DC metropolitan area travel or living expenses will be allowed under this contract.

# F.3 DELIVERABLES AND DELIVERY SCHEDULE

The following schedule of milestones will be used by the COR to monitor timely progress under this Call Order.

The following abbreviations are used in this schedule:

DEL: Deliverable

IAW: In Accordance With

NLT: No Later Than

TOA: Call Order Award

TBD: To Be Determined

All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

|  |  |  |
| --- | --- | --- |
| **TASK** | **Deliverables** | **Tentative Date Due** |
| **TASK 1**  Set-up and Implement SWIFT  Mail Digitization  **TASK 2**  Develop, Deploy, and  Implement SWIFT Digital Mail Stop Delivery | * Mail scanning integrated with SWIFT * SWIFT scanning intake personnel trained and supported through implementation * Fully Implemented SWIFT Solution supporting the implementation of digital mail stops with second-level delivery and return request functionality * Integration of the new SWIFT Digital Mail application with the existing SWIFT Executive Correspondence application SWIFT Digital Mail Stop, POCs trained and supported through implementation * Monthly status reports * System Documentation * User Manual * End User Training | Monthly status reports due on 10th of each month |
| **OPTIONAL TASK 3**  Annual Technology Refresh | * Fully Implemented SWIFT Solution to support digital delivery of scannable Accountable or Certified Mail Staff trained on usage of the SWIFT Accountable Mail functionality * Monthly status reports * System Documentation * User Manual * End User Training | Monthly status reports due on 10th of each month |

**The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government’s data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with**

# F.4 DELIVERY REQUIREMENTS

The contractor shall submit deliverables that are clear, concise, and complete, and that conform to standards that shall be agreed to in advance between the Contractor and the Project Officer.

Delivery schedule shall be agreed upon in advance between the Contractor and Project Officer.

All documentation will be submitted in the following format and quantity: • One (1) camera-ready copy (for reproduction by ACF)

• One (1) electronic copy in Word format.

ACF will have five (5) working days to review each deliverable and accept or reject the deliverable in writing. Any deliverable product under this contract will be accepted or rejected in writing by the Project Officer. The Project Officer will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the contractor’s accepted proposal. In the event of rejection of any deliverable, the contractor will be notified in writing by the Project Officer of the specific reasons why the deliverable is being rejected. The contractor shall have five (5) working days to correct the rejected deliverable and resubmit it to the Projector Officer.

The Contractor shall submit all required report(s)/deliverables in accordance with the schedule(s) outlined in the SOW and the Deliverable Table above. All reports shall reference and cite the contract/order number. The Contractor will provide all deliverables to the COR. All draft deliverables will be delivered in an editable format, such as Microsoft Word, and submitted electronically; all final deliverables will be delivered electronically in an editable format, including embedded images (e.g. Microsoft Word, Excel, Visio, Project, Adobe Acrobat, XML, etc.) or other electronic format as prescribed by the COR. The Contractor shall use ACF governance-provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate; if specific formats are not provided, the Contractor shall deliver in its own format, as appropriate.

In compliance with Section 508 of the Rehabilitation Act, final deliverables that include graphics (e.g., pie charts, bar graphs, etc.) will include a separate Microsoft Word file identifying the page, exhibit number/name, and narrative text in the deliverable. The Contractor shall not release or post live materials on any website or in any publication until after the deliverable is officially released by ACF. The Contractor shall use provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate; if specific formats are not provided, the Contractor shall deliver in its own format, as appropriate.

# F.5 DELIVERABLE ACCEPTANCE

The contractor shall submit deliverables that are clear, concise, and complete, and that conform to standards that shall be agreed to in advance between the Contractor and the COR. Delivery schedule shall be agreed upon in advance between the Contractor and COR.

OES will have five (5) working days to review each deliverable and accept or reject the deliverable in writing. Any deliverable product under this contract will be accepted or rejected in writing by the COR. The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the contractor’s accepted quote. In the event of rejection of any deliverable, the contractor will be notified in writing by the COR of the specific reasons why the deliverable is being rejected. The contractor shall have five (5) working days to correct the rejected deliverable and resubmit it to the COR.

# SECTION G. CONTRACT ADMINISTRATION DATA G.1 AUTHORITIES OF GOVERNMENT PERSONNEL

Notwithstanding the Contractor’s responsibility for total management during the performance of this contract, the administration of the contract will require coordination between the

Government and the Contractor. The following individuals will be the Government’s points of contact during performance of the contract.

# Contract Specialist

Tifanie Lewis

U.S. Department of Health and Human Services

Administration for Children and Families

Office of Government Contract Services

330 C Street S.W. Room

Washington, DC 20201

Phone: 202-690-7807

Email: Tifanie.Lewis@acf.hhs.gov

# Contracting Officer

Julius Bradshaw

U.S. Department of Health and Human Services

Administration for Children and Families

Office of Government Contract Services

330 C Street S.W. Room

Washington, DC 20201

Phone: 202-568-9131

Email: Julius.Bradshaw@acf.hhs.gov

# Contracting Officer's Representative (COR)

Rudette Pinkney

Administration for Children & Families (ACF)

Office of Executive Secretariat

330 C Street S.W. Room 4020A

Washington, DC 20201

Phone: (202)401-0527

Email: Rudette.Pinkney@acf.hhs.gov

Note: The Contracting Officer is the only individual authorized to modify this requirement.

# G.2 TECHNICAL MONITORING

Performance of the work under this contract shall be subject to the technical monitoring of the COR. The term “Technical Monitoring” is defined to include, without limitation, the following:

Technical directions to the Contractor that redirect the contract effort, shift work emphasis between work areas or assignments, require pursuit of certain lines of inquiry, fill in details or otherwise serve to accomplish the contractual scope of work.

Providing information to the Contractor for assistance in the interpretation of drawings, specifications or technical portions of the work description.

Review and, where required by the contract, approval of technical reports, drawings, specifications and technical information to be delivered by the Contractor to the Government under the contract.

Technical direction must be within the general scope of the work stated in the contract. The COR does not have authority to and may not issue any technical direction which:

* Constitutes any assignment of additional work outside the general scope of the contract.
* Constitutes a change as defined in the contract clause entitled, “Changes”.
* In any manner causes an increase in the total contract cost or the time required for contract performance; or
* Changes any of the expressed terms, conditions, or specifications of the contract.

All technical directions shall be issued in writing by the COR or shall be confirmed by him/her in writing with five (5) working days after issuance.

The Contractor shall proceed promptly with the performance of technical directions duly issued by the Project Officer in the manner prescribed within his authority under this provision. If, in the opinion of the Contractor, any instruction or direction issued by the COR is within one of the categories as defined in (i) through (iv) above, the Contractor shall not proceed, but shall notify the Contracting Officer in writing within five (5) working days after the receipt of any such instruction or direction and shall request the Contracting Officer to modify the contract accordingly. Upon receiving such notification from the Contractor, the Contracting Officer shall issue an appropriate contract modification or advise the Contractor in writing that, in his/her opinion, the technical direction is within the scope of this article and does not constitute a change under the Changes Clause of the contract. The Contractor shall thereupon proceed immediately with the direction given. A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto shall be subject to the provisions of the contract clause entitled, “Disputes”.

# G.3 GOVERNMENT -FURNISHED PROPERTY

Badges and Government Laptops are needed for this acquisition. The furnished property will be provided upon awarding of the contract.

**G.4 GOVERNMENT -FURNISHED INFORMATION**

Government Furnished Information is not anticipated for this acquisition.

# G.5 INVOICES

The Contractor shall submit invoices once per month. A complete invoice with all required backup documentation shall be sent electronically, via email, to:

1. Contract Specialist via Tifanie.lewis@acf.hhs.gov.
2. Contracting Officer's Representative (COR): rudette.pinkney@acf.hhs
3. Financial Management Service (FMS): psc\_invoices@psc.hhs.gov.
4. Business Manager: linda.hitt@acf.hhs.gov

\* No other non-invoice related documents (i.e. deliverables, reports, balance statements) shall be sent to the DAM and FMS mailboxes. Invoices Only.

The Contractor shall include the following minimum information on invoices:

1. Contractor's name and invoice date;
2. Contract number or other authorization for delivery of property or services;
3. Description, price, and quantity of property or services actually delivered or rendered;
4. Shipping and payment terms;
5. Other substantiating documentation or information as required by the contract;
6. Name (where practicable), title, telephone number, and complete mailing address of responsible official to whom payment is to be sent;
7. The Internal Revenue Service TAX IDENTIFICATION NUMBER; and
8. Signature of an authorized official certifying the invoice to be correct and proper for payment.
9. Call Order #: 75P0011A00091/75ACF121F80047

Payment shall be made by:

PSC/Financial Management Service

Division of Financial Operations

Parklawn Building, Room 16A-12

5600 Fishers Lane

Rockville, Maryland 20857

**FOR INVOICE STATUS CALL**: (301) 443-3020

# Payment by Electronic Funds Transfer

Pursuant to FAR 52.232-33, Payment by Electronic Funds Transfer –Central Contractor Registration, payments under this contract shall be made by electronic funds transfer. The Contractor shall register in the Central Contractor Registration database.

**SECTION H. SPECIAL CONTRACT REQUIREMENTS**

# H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this TO.

1. Project Manager
2. System Architect
3. System Engineer
4. System Analyst
5. Software Engineer

The Government desires that Key Personnel be assigned for the duration of the Call Order.

# H.1.1 PROGRAM MANAGER

It is desired that the project manager has the following qualifications:

1. Specialize in developing, delivering, and supporting case management and workflow solutions for government agencies

1. Manage government contracts to deliver new solutions/platforms, operations, maintenance, modernization, and best practices.

1. Manage agency-wide administrative management Information Technology (IT) applications projects that integrate, track, and manage files consisting of executive correspondence, rules, and regulations.

1. Manage project budgets, write proposal, and project plans, manage project requirements, and apply best practices for government contracts

# H.1.2 SYSTEM ARCHITECT

It is desired that the System Architect has the following qualifications:

1. Design activities and technical collaboration for enterprise-wide correspondence and interagency agreements systems within the government

1. Design data warehouse for reporting and analytics

1. Manage all aspects of the development and integration of government client-server workflow

solutions; including requirements analysis, solution systems design, and development Implementation, and post-implementation support.

# H.1.3 SYSTEM ENGINEER

It is desired that the Software Engineer has the following qualifications:

1. Led development teams in implementing and maintenance of custom based applications as well as integrations with off the shelf products for the government.

1. Monitor existing government systems to ensure structural integrity, oversee the development and installation of new hardware and software, install and configure operating systems, software, and routinely test installed software for glitch detection and other issues.

# H.1.4 SYSTEM ANALYST

It is desired that the System Analyst has the following qualifications:

1. Manages service desk technical support for several government applications

1. Perform error debugging and investigate complex issues from government once detailed information had been provided.

1. Monitor government system servers, components, services, as well as monthly maintenance, data charts, tracking, and database auditing.

# H.1.5 SOFTWARE ENGINEER

It is desired that the Software Engineer has the following qualifications:

1. Design and develop software solutions on the Microsoft .NET framework using a wide range of technologies for the government

1. Design and implement multiple solutions integrating the SWIFT platform with external Systems

**2.** Oversees management and execution of several quality code releases to government

# H.2 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the COR. Prior to utilizing other than the Key Personnel specified in its proposal in response to the Call Order Request , the contractor shall notify the COR. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on Call Order performance. Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the Call Order, the contractor may be subject to default action as prescribed by FAR 52.249-6

Termination *(Cost Reimbursement) or* FAR 52.249-8, Default *(Fixed-Price Supply and Service).*

# H.3 BASELINE SECURITY REQUIREMENTS

**H.3.1. Applicability.**

The requirements herein apply whether the entire contract or order (hereafter “contract”), or portion thereof, includes either or both of the following:

1. 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.

1. 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.

# H.3.2 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:

1. 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.

1. 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.

1. 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.

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

# H.3.3 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.

# H.3.4 CONTROLLED UNCLASSIFLIED 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:

1. marked appropriately;

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

1. 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

1. 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 80088*, Guidelines for Media Sanitization*.

# H.3.5 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.

# H.3.6 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 ACFpolicies. Unauthorized disclosure of information will be subject to the HHS/ACF sanction policies and/or governed by the following laws and regulations:

1. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);

1. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and

1. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

# H.3.7 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)*.

# H.3.8 WEBSITES AND DIGITAL SERVICES

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

# H.3.9 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.

# H.3.10 CONTRACT DOCUMENTATION

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

# H.3.11 STANDARD FOR ENCRTPTION

The Contractor (and/or any subcontractor) shall:

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

1. 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.

1. 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).

1. 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.

1. 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.

# H.3.12 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.

# H.3.13 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.

1. 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*.
2. 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.

# H.4 ELECTRONIC INFORMATION AND TECHNOLOGY ACCESSIBILITY NOTICE (December 1, 2015)

(a). Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the

Workforce Investment Act of 1998 and the Architectural and Transportation Barriers

Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain, or use electronic and information technology, 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, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

1. Accordingly, any offeror responding to this solicitation must comply with established HHS

EIT accessibility standards. Information about Section 508 is available at [http://www.hhs.gov/web/508.](https://www.hhs.gov/web/508) The complete text of the Section 508 Final Provisions can be accessed at [http://www.access-board.gov/guidelines-and-standards/communications-andit/about-the-section-508-standards*.*](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards)

1. The Section 508 accessibility standards applicable to this solicitation are listed below: [https://www.hhs.gov/web/section-508/making-files-accessible/checklist/index.html**.**](https://www.hhs.gov/web/section-508/making-files-accessible/checklist/index.html)In order to facilitate the Government’s determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors 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 offerors 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 on the HHS website [http://www.hhs.gov/web/508.](https://www.hhs.gov/web/508) In order to facilitate the Government’s determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors 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.

1. Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

**H.5 TRAINING**

# H.5.1 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/ACFInformation 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.

# H.5.2 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*.

# H.5.3 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.

# H.6 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.

# H.7 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.

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

1. 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.
2. 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.

# H.7 POSITION SENSITIVIY 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: Information Technology – Non-Critical Sensitive **Roster.** The Contractor (and/or any subcontractor) shall submit a roster by name, position, email 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 daysof the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 24 hoursof 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.

# H.8 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)](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)](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.](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-securityprivacy-program/index.html.](https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/information-security-privacy-program/index.html)

**H.9 CONTRACT INITIATIONAND EXPIRATION**

# H.9.1 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.

# H.9.2 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.

# H.9.3 SANITATION 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*.

# H.9.4 NOTIFICATION

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

# H.9.5 CONTRACTOR RESPONSIBILITIES UPON PHISICAL 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.

# H.9.6 CONTRACT STAFFING

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

# H.10 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*/*ACFpolicies 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.

# H.11 OPERATIONS AND MAINTENANCE FOR FEDERAL IT SYSTEM

The Contractor shall monitor, manage, assess, and report on the SWIFT 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 SWIFT 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 SWIFT. 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

# H.11 HOSTING OF FERDERAL 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

SWIFT. 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

# H11.1 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.

# H.11.2 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 800¬37, 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).

# H.11.3 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:

1. 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.

1. 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.

1. 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.

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

# H.11.4 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.

# H.11.5 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:

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

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

1. 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;

1. 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

1. 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.

# H.11.6 DEVELOPMENT, MODERIZATION AND ENHANCEMENT

The purpose of this task is to provide development, modernization and enhancement to the SWIFT. 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 nonfunctional 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.

1. 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.

1. 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.

1. 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.

1. 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);

1. Has a consistent appearance;

1. Does not overlap with or duplicate any legacy websites and, if applicable, ensure that legacy websites are regularly reviewed, eliminated, and consolidated;

1. Contains a search function that allows users to easily search content intended for public use; 5) Is provided through an industry standard secure connection;

1. 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;

1. 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

1. Is fully functional and usable on common mobile devices.

**H.12 CONTRACT TRANSITION MANAGEMENT**

# H.12.1 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:

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

# H.12.2 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

# H.12.3 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 Call 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, resourceplanning/resource turnover analysis, travel cost

# H.13. RECORDS MANAGEMENT

1. 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.

1. 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:

* + Includes ACF records.
  + Does not include personal materials.
  + Applies to records created, received, or maintained by Contractors pursuant to their ACF contract.
  + May include deliverables and documentation associated with deliverables.

1. Requirements

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)

1. 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.

1. Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

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

1. Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

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

1. 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.

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

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.

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.

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.

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).

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.

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.

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.

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.

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.

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

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.

Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

# H.14 QAULITY ASSURANCE SERVEILLANCE 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.

**H.15 508 ACCESSIBILITY STANDARDS**

# 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-andpolicies.

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/aboutthe-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-thesection-508-standards/section-508-standards#subpart\_c](https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards#subpart_c)

**352.239-73 Electronic Information and Technology Accessibility Notice.**

(a) As prescribed in [HHSAR 339.203-70(a),](https://www.hhs.gov/node/4249#339.203-70) the Contracting Officer shall insert the following provision:

Electronic and Information Technology Accessibility Notice (December 18, 2015)

1. Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the

Workforce Investment Act of 1998 and the Architectural and Transportation Barriers

Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain, or use electronic and information technology, 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, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

1. Accordingly, any offeror responding to this solicitation must comply with established HHS

EIT accessibility standards. Information about Section 508 is available at [http://www.hhs.gov/web/508.](http://www.hhs.gov/web/508) The complete text of the Section 508 Final Provisions can be accessed at [http://www.access-board.gov/guidelines-and-standards/communications-andit/about-the-section-508-standards*.*](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards)

1. The Section 508 accessibility standards applicable to this solicitation are stated in the clause at [352.239-74,](https://www.hhs.gov/node/4251#352.239-74) Electronic and Information Technology Accessibility.

In order to facilitate the Government’s determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors 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 offerors 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 on the HHS website [http://www.hhs.gov/web/508.](http://www.hhs.gov/web/508)

In order to facilitate the Government’s determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors 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.

1. Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

## (End of provision)

**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 Contractor 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,](https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule) 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.**

o 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.

# o 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-StandardsSafe-Harbor-and-FAR-Update**](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, quoter 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 quoter 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, quoter 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.

1. 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)](https://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.

1. 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

# H. 16 Data Rights

The Government has unlimited rights to all documents/material produced under this Call 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.

**SECTION I. CONTRACT CLAUSES FEDERAL ACQUISITION REGULATIONS (FAR) 48 CFR CHAPTER CLAUSES**

All other terms and condition in the parent contract apply herein.

# I.1. DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION

**REGULATION (HHSAR) (48 CFR Chapter 3) Contract Clauses**

|  |  |  |
| --- | --- | --- |
| **CLAUSE** | **TITLE** | **DATE** |
| 352.224-70 | Privacy Act | December 2015 |
| 352.237-75 | Key Personnel | December 2015 |
| 352.239-73 | Standard for security configurations | December 2015 |
| 352.270-11 | Protection of Human Subjects—Research Involving  Human Subjects Committee (RIHSC) Approval of Research Protocols Required | December 2015 |

# SECTION J. LIST OF ATTACHMENTS

|  |  |
| --- | --- |
| Attachment A. | Contractor Non-Disclosure Agreement |
| Attachment B. | List of Deliverables |