SECTION C – DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1. BACKGROUND

SWIFT is a mission critical application that IOS continues to rely on to route and track correspondences within HHS. SWIFT currently resides at the Government Transformation Center (application hosting facility) in Reston Virginia and at the Hubert Humphrey building in Washington, DC. Due to the award of the new IT services IDIQ contract for HHS employees, IOS must provide IT services to assist with setting up and migrating two logical servers and one virtual server at the Information Innovators Inc., Triple-I site located in Reston VA.

C.2. 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).

C.3. OBJECTIVES

The objective of this Statement of Work (SOW) is to obtain IT services in the area of end user support from Sole Solution Inc. to support the operation of the correspondence control process F

C.4. DELIVERABLE

C.4.1. TASK I – END USER SUPPORT

The SWIFT End User Support the services provided to ACF consists of the following services:

- Daily and real-time system monitoring by SWIFT technicians
- Provide a total of 110 hours of on- site support within the contract period. Support services will be located at the Switzer building in Washington DC.
- Daily offsite support for all SWIFT users
- Support will be provided Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m. EST.
- Support requests will be submitted to the SWIFT Support Desk via email, or in person to onsite personnel.
- Resolution of user support requests and inquiries
- Hands-on training for new users
- Monthly status reports from the project manager
- EPIC Workfolder License: Requires the acquisition a license of the SWIFT Epic Workfolder product. The license is a multi-tenant, single-server license; shared between multiple tenants hosted on a single server which provides for an unlimited number of SWIFT users.
- Data Storage Reduction (Archive). The Contractor will remove specified files from the SWIFT system and will make the files available in ZIP format for download by ACF. The specific requirements that define which files will be moved as outlined with the user. The Contractor will perform this task only once during the period of performance.

.

Deliverables**:**

- 12 months of End User Support
- Monthly status reports
- EPIC License
- Move selected SWIFT files to ACF file archive
- Delete selected files from SWIFT

C.4.2. TASK 2 – ANNUAL TECHNOLOGY REFRESH

The Contractor will maintain an application development capability to provide one application upgrade each year to resolve potential system compatibility issues with new versions of Microsoft Internet Explorer, Microsoft Office, and Microsoft Windows.

SWIFT is a .Net application consisting of components from many vendors including Microsoft, Adobe, Infragistics and Data Dynamics. The progress of technology is inevitable, but predictable, and new versions of these products are released every 12-18 months. The purpose of the Annual Technology Refresh is to ensure that SWIFT remains compatible with upgrades of user desktops with new software and operating systems.

The Contractor will meet the following requirements:

- In preparation for the annual technology refresh of the SWIFT application, the Contractor will meet with the Contracting Officer's Representative (COR) to discuss the Government's schedule for release of new versions of Microsoft Internet Explorer, Microsoft Office, and Microsoft Windows. The COR may also request that the Contractor address specific minor software errors that affect users' ability to use existing features of the application.
- Based on the information provided by the COR, the Contractor will prepare an Annual Technology Refresh plan detailing the items to be addressed. If the Contractor is unable to address a specific software error, the Contractor will provide an appropriate alternative or justification.
- The Contractor will provide all the software and equipment necessary to verify the compatibility of the SWIFT application with new versions of the Microsoft desktop products in their own facility.
- The Contractor will provided updated user documentation for any significant change to the application user interface or functionality.

In order to obtain the best quote from the Contractor for this task, the scope of the Annual Technology Refresh effort will not include the following:

- Installation of the SWIFT application on new server hardware.
- Significant application updates in response to network or infrastructure upgrades or modification.

- Significant application updates to meet new Agency software architecture guidelines, or security requirements. The objective of this task is software compatibility, not policy compliance.
- Application updates to implement new features, business logic or data validation.
- Application updates to replace integrated third party components that are no longer supported by the vendor.
- Installation of updated versions of applications licensed directly to the Government and used with the SWIFT system, such as third party reporting tools, SQL Server, and Adobe Acrobat.
- Participation in system security testing and modification of the SWIFT application in response to security testing.
- Enabling new SWIFT functionality developed for other clients that require significant process analysis or configuration effort.
- Install or maintenance of a test or validation environment at HHS. Test and validation environments are maintained at the SSI facility.

Deliverables:

- Annual Technology Refresh

C.4.3. TASK 3 End User Reporting

SWIFT contains workflow data that is important to management decisions made by ACF leadership. SWIFT provides tools to search and extract data (e.g. Advanced Search) but these tools do not aggregate or group data and significant effort is required on the part of ACF staff to manually summarize data in a meaningful way.

ActiveReports Server was made available to ACF with more advanced reporting features. The tool was configured to pull information from a dedicated SWIFT reporting repository that orders and simplifies complex SWIFT data for more consistent reporting.

SSI trained two advanced reporters at ACF who have the capability to create new reports in the ActiveReports Server and to schedule automatic delivery of those reports to email recipients. SSI also gave limited read-only access to the tool to other staff. As part of this task, SSI will continue to provide training and assistance to two (2) advance reporters and up to ten (10) read- only access users upon request throughout the period of performance of this project.

Creating reports is a complex task and requires users have an extensive understanding of SWIFT data relationships and common report creation concepts such as grouping and filtering. Limiting the number of users who have access to this tool will enable SSI to provide a competitive quote.

The following activities are included in this task:

- The Contractor will maintain the ActiveReports data warehouse. This includes daily integrity checks to verify that the nightly refresh of the reporting data repository processed correctly and resolution of any user reported issues.
- The Contractor will monitor and maintain the licensed ActiveReports server components in a manner that is consistent with HHS information security policy.
- The Contractor will perform upgrades of the ActiveReports server components as necessary to maintain compatibility with the server environment and workstation browser software versions.
- The Contractor will provide ongoing training to up to two ACF staff "reporters" who will design and deploy reports for up to ten ACF staff members who will have read-only access to ActiveReports.
- The Contractor will provide ongoing onsite and remote support as necessary to the two ACF staff "reporters" to assist them in the definition, design and deployment of new reports.
- The Contractor will add simple calculations as new attributes to the ActiveReports repository as necessary to support the creation of new reports.

Deliverables:

- ActiveReports training and support.

C.4.4. Task 4 Two (2) Formal Training Sessions

The Contractor will provide two (2) customized training programs, with follow-up. The Contractor will prepare and conduct the customized training program using the following procedure:

- After the award, the Contractor will meet with the Contracting Officer's Representative (COR) and primary SWIFT stakeholders to prepare a high-level plan for the customized user training. This plan should include the approximate time table and target audience for each session.
- In preparation for each customized training program, the Contractor will meet with the Contracting Officer's Representative (COR) and primary SWIFT stakeholders to discuss the overall goals. The Contractor will present at the meeting some possible topics for consideration based on their analysis of the system data and process maps. The primary SWIFT stakeholders will provide direction to the Contractor.
- The Contractor will interview key users who will be present at the training. This meeting will provide the Contractor an opportunity to understand the user's internal processes, clarify specific system use questions, and prepare for user questions that may be presented during training.
- The Contractor will prepare a training script and slides to address the issues and goals identified above.
- Each user training session shall be 1.5 to 2 hours long. Each training program can include up to two identical sessions, scheduled within a week of one another. No special training environment or user accounts will be configured

by the Contractor as part of this effort. This estimate is based upon the assumption that the Contractor will conduct user interviews and the training program with onsite support hours. Data analysis and training program preparation will take place at the Contractor's facility.

- After the training is complete, the Contractor will analyze the system to determine the effectiveness of the training and will present their findings to the COR and primary SWIFT stakeholders.
- The Contractor shall provide updated user manuals at the training sessions. An electronic version of the manuals shall be provided to the COR.

Deliverable:

- Two (2) formal training sessions

C.4.5. Task 5 Server Upgrade

ACF uses SWIFT application to manage many types of files associated with the correspondence process including original correspondence, multiple response drafts, clearance comments and other tenant agencies is hosted on three servers in the MAHC Data center in Reston, VA maintained by Sev 1 Tech. These servers are currently configured with Windows Server 2008, and Microsoft will no longer support the operating system after January of 2020. The SWIFT servers need to be updated to Windows Server 2016 and SQL Server Enterprise 2016.

The Contractor shall implement the enhancements listed below on the Documents tab and the task form.

- The Contractor will reinstall SWIFT on servers that have been upgraded to Windows Server 2016. SWIFT will be thoroughly tested by the Contractor after the installation to ensure proper functioning.

- All necessary hardware and Windows Server 2016 and SQL Server license will be provided by the Government.

Deliverables:

- **Reinstallation of SWIFT on new server**
- **Testing of SWIFT application on server**

C.4.6. Task 6 Data Entry- Primary Action (Direct Reply with Clearance Tab)

ACF uses the Action Required tab on the Data Entry screen to assign a primary action to the correspondence that is being delivered to the program office from SWIFT. The Direct Reply with Clearance tab will notify the program office that the correspondence attached to the SWIFT task needs a direct reply response, but the response must go through the clearance process before it can be mailed out from ACF to the writer of the correspondence.

- The Contractor will implement the necessary actions to install the direct reply with clearance tab on the data entry screen under the primary action section.

Deliverables:

- **Install a new direct reply with clearance tab on data entry screen**

C.4.7. Task 7 Data Entry- Status Tab (Clearance Review)

ACF uses the Status tab on the Data Entry screen to assign the status of a correspondence in SWIFT. The status tab provides the status of the correspondence in SWIFT so the analyst will know how to process the task. The contract will change the way the Clearance review tab functions. Currently, when a task is sent to multiple program offices; the status changes on the task once the last program office submits their response. We are requesting the status changes when the first program office submits their response.

- The Contractor will implement the necessary actions to change the clearance review tab function on the data entry screen under the status tab.

Deliverables:

- **Change the clearance review function on the status tab to change the clearance review tab function on the data entry screen under the status tab**

C.5. BASELINE SECURITY REQUIREMENTS

C.5.1.Applicability**.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.

b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS 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.

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

a. Protect government information and information systems in order to ensure:
   - **Confidentiality**, which means preserving authorized restrictions on access and

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

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, **within one (1) hour or less**, bring the situation to the attention of the other party.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

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

2) **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 are the following:

Confidentiality:	[ ] Low [X] Moderate [ ] High
Integrity:	[ ] Low [X] Moderate [ ] High
Availability:	[ ] Low [X] Moderate [ ] High
Overall Risk Level:	[ ] Low [X] Moderate [ ] High

Based on information provided by the ISSO, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[X] No PII [ ] Yes PII

3) **Confidentiality and Nondisclosure of Information.** Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS 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 HHS 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 policies. Unauthorized disclosure of information will be subject to the HHS sanction policies and/or governed by the following laws and regulations:

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

4) **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)*. .

5) **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.

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

*See **Attachment 1.** List of Deliverables*

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

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

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

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and

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

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

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

8) **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. , as applicable. 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.

See Attachment 2 for the HHS Contractor Non-Disclosure Agreement.

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

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

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

C.5.2. Training

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

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

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

C.5.3. 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 HHS 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 above.

C.5.4. Incident Response

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC) IRT teams **within 24 hours,** whether the response is positive or negative.

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 HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an

other than authorized purpose. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines a breach as "a suspected or confirmed incident involving PII" .

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 with FIPS 140-2 validated encryption.

2) NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send ACF approved notifications to affected individuals.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the ACF Incident Response Team (IRT) , COR, CO, ACF SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

   a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;

   b. not include any sensitive information in the subject or body of any reporting e-mail; and

   c. encrypt sensitive information in attachments to email, media, etc.

4) Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* HHS incident response policies when handling PII breaches.

5) 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 .

C.5.5 Position Sensitivity Designations

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

Security Level is Medium-low

C.5.5 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.*

.

For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential-directive-12)

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within 5 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 5 days of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member

If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

C.5.6, Contract Initiation and Expiration

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 framework and methodology in accordance with the HHS Contract Closeout Guide (2012).

HHS EA requirements may be located here:
https://www.hhs.gov/ocio/ea/documents/proplans.html

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

require artifact review and approval.

3) **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 5 days before an employee stops working under this contract.

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

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the Contractor Employee Separation Checklist when an employee terminates work under this contract within 5 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

C.5.7. Records Management and Retention

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

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

SECTION D – PACKAGING AND MARKING

SECTION E – INSPECTION AND ACCEPTANCE

E.1. INSPECTION AND ACCEPTANCE

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 Technical Representative (COTR) 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.2. APPROVALS BY THE COTR

All services delivered to the COTR 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 COTR's approval or revision to the services delivered shall be within the general scope of work stated in this contract.

E.3. FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://www.arnet.gov/far/

CLAUSE	TITLE	DATE
52.246-4	Inspection of Services –Fixed Price	August 1996
52.246-6	Inspection – Time-and-Materials and Labor hour	May 2001

SECTION F – DELIVERIES OR PERFORMANCE

F.1. DELIVERABLES/DELIVERY SCHEDULE

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 HHS)
- One (1) electronic copy in Word format.

IOS 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.

TASK	Deliverables	Tentative Date Due
TASK I - *SWIFT End User Support*	• SWIFT Support • Monthly status reports • EPIC License • Move selected SWIFT files to ACF file archive • Delete selected files from SWIFT	Monthly status reports due on 10th of each month Note: Epic License October 15 2018 Archive and Delete Deliverables(July 31
TASK II – *Annual Technology Refresh*	• Annual Technology Refresh	September 15, 2018
TASK III -*End-User Reporting*	• ActiveReports maintenance and training	September 15, 2018
TASK IV *– Two (2) Formal Training Sessions*	• Two (2) formal training sessions	September 15, 2018
TASK V - *File Management Enhancements*	• Redesigned "More Files" dialog • Enhance the Documents tab with version history • Enable a flag for files in Documents tab and More Files dialog	December 15, 2017
TASK VI –*Change Default Due Date for the Approval Task Type*	• Update Approval Task default date	November 15, 2017
TASK VII –*Electronic Approval Package*	• Electronic Approval Package • Electronic signature applet	January 15, 2017

F.2. PERIOD OF PERFORMANCE

The period of performance is a based period of 6 months. Any extension to the below period of performance shall be approved by the Contracting Office and Project Officer prior to the extension.

Base Period: September 30, 2017 through September 29, 2018

F.3. PLACE OF PERFORMANCE

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

1.	New Year's Day	January 1st
2.	Martin Luther King's Birthday	Third Monday in Jan.
3.	President's Day	Third Monday in Feb.
4.	Memorial Day	Last Monday in May
5.	Independence Day	July 4th
6.	Labor Day	First Monday in Sept.
7.	Columbus Day	Second Monday in Oct.
8.	Veteran's Day	November 11
9.	Thanksgiving Day	Fourth Thursday Nov.
10.	Christmas Day	December 25

F.5. FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://www.arnet.gov/far/

CLAUSE	TITLE	DATE
52.242-15	Stop-Work Order	August 1989
52.242-17	Government Delay of Work	March 2014

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.

1. Contracting Officer

All contract administration shall be done by:

All communications pertaining to contractual and/or administrative matters under the contract shall be sent to the address above and to the attention of:

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

2. Primary Contracting Officer's Representative (COR)

Yolanda Santiago
Administration for Children & Families (ACF)
Office of Administration
Office of Management Operations
330 C Street S.W. Room 3109B
Washington, DC 20201
Phone: (202)690-5789
Email: Yolanda.Santiago@acf.hhs.gov

Secondary Contracting Officer's Representative (COR)

Rudette Pinkney

Administration for Children & Families (ACF)

Office of the Assistant Secretary

330 C Street S.W. Room 3109B

Washington, DC 20201

Phone: (202)401-0527

Email: Rudette.Pinkney@acf.hhs.gov

Technical Monitoring

Performance of the work under this contract shall be subject to the technical monitoring of the COTR. 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 COTR 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 COTR 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 COTR 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.2. INVOICE SUBMISSION

The Contractor shall submit an ORIGINAL invoice including supporting documentation on a **monthly** basis to the below address and the COTR:

Division of Acquisition Management/Program Support Center
Attention: Antony Terrell
Parklawn Building, Room 5-101
5600 Fishers Lane
Rockville, Maryland 20857
BPA #:
BPA Call Number:

The Contractor shall submit one (1) copy of the invoice including (1) copy of supporting documentation on a **monthly** basis, to:

PSC/Financial Management Service
Division of Financial Operations
Parklawn Building, Room 16A-12
5600 Fishers Lane
Rockville, Maryland 20857
BPA #:
BPA Call Number:

1. 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.

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

H.1 (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.

(b) 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. The complete text of the Section 508 Final Provisions can be

accessed at http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards.

(c) 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.

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.

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.

(d) 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.

SECTION I – CONTRACT CLAUSES

FEDERAL ACQUISITION REGULATIONS (FAR) 48 CFR CHAPTER CLAUSES

I.1. SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FAR 52.252-1, FEBRUARY 1998) & CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2, FEBRUARY 1998)

This contract incorporates some FAR provisions/clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://www.arnet.gov/far/index.html. The applicable provisions/clauses are as follows:

CLAUSE	TITLE	DATE
52.202-1	Definitions	July 2004
52.203-3	Gratuities	April 1984

52.203-5	Covenant Against Contingent Fees	April 1984
52.203-7	Anti-Kickback Procedures	July 1995
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	January 1997
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	January 1997
52.215-8	Order of Precedence--Uniform Contract Format	October 1997
52.216-31	Time & Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition	February 2007
52.217-8	Option to Extend Services	November 1999
52.227-14	Rights in Data	December 2009
52.232-18	Availability of Funds	April 1984
52.232-25	Prompt Payment	October 2008
52.233-2	Service of Protest	August 1996
52.233-4	Applicable Law for Breach of Contract Claim	October 2004
52.243-1	Changes – Fixed-Price	April 1987

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

I.2. DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR Chapter 3) Contract Clauses

CLAUSE	TITLE	DATE
352.202-1	Definitions	January 2006
352.224-70	Confidentiality of Information	January 2006
352.232-9	Withholding of Contract Payments	January 2006
352.233-70	Litigation and Claims	January 2006
352.239-70	Standard for security configurations	September 2009
352.249-14	Excusable Delays	January 2006
352.270-6	Publications and Publicity	January 2006
352.270-7	Paperwork Reduction Act	January 2006
352.270-11	Privacy Act	January 2006

Attachment 1. List of Deliverables

The following table details a listing of possible deliverables that may be completed by the contractor (at a minimum) and included in the Schedule of Deliverables *[OpDiv specify process/format for submitting deliverables]*. **Please note that deliverables from section 2 apply to sections 3, 4, and 5.**

Document Section	Deliverable Title/Description	Due Date	Applicable (y/n)
2 – Roster	Roster	Within *[OpDiv-specific timeline]* of the effective date of this contract	
2 – Contractor Employee Non-Disclosure Agreement (NDA)	Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS	
2 – Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)	Assist in the completion of a PTA/PIA form	Within *[OpDiv insert contract-specific timeline]* after contract award	
2 – Training Records	Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request	
2 – Rules of Behavior	Signed ROB for all employees	Initiation of contract and at least annually thereafter	
2 – Incident Response	Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery	
2 – Incident Response	Incident and Breach Response Plan	Upon request from government	
2 – Personnel Security Responsibilities	List of Personnel with defined roles and responsibilities	Within *[OpDiv-specific timeline]* that is before an employee begins working on this contract.	
2 – Personnel Security Responsibilities	Off-boarding documentation, equipment and badge when leaving contract	Within *[OpDiv-specific timeline]* after the Government's final acceptance of the work under this contract, or in the	

Document Section	Deliverable Title/Description	Due Date	Applicable (y/n)
		event of a termination of the contract.	
2 – Background Investigation	Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS	
2 - Certification of Sanitization of Government and Government Activity-Related Files, Information, and Devices.	Form or deliverables required by OpDiv.	At contract expiration. *[OpDiv-specific]*	
2 – Contract Initiation and Expiration	If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration. *[OpDiv-specific]*	
4 – Security Assessment and Authorization (SA&A)	SA&A Package • SSP • SAR • POA&M • Authorization Letter • CP and CPT Report • E-Auth (if applicable) • PTA/PIA (if applicable) • Interconnection/Data Use Agreements (if applicable) • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other OpDiv-specific documents	Due within *[insert contract-specific timeline]* after contract award.	
5 – Protection of Information in a Cloud Environment	Contract expiration	Due within *[insert contract-specific timeline]* after contract award.	
5 – SA&A Process for Cloud Services	SA&A Package • SSP • SAR	Due within *[insert contract-specific timeline]* after contract	

Document Section	Deliverable Title/Description	Due Date	Applicable (y/n)
	• POA&M • CMP • CP and CPT Report • E-Auth (if applicable) • PTA/PIA (if applicable) • Penetration Test Results • Interconnection/Data Use/Agreements (if applicable) • Service Level Agreement • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other OpDiv-specific documents	award.	
5 – Reporting and Continuous Monitoring	POA&M updates; Revised security documentation/Agreements	Monthly/as requested by OpDiv	
5 – Security Alerts, Advisories, and Directives	List of personnel with designated roles and responsibilities	OpDiv-Specified	
5 – Incident Reporting	• Incident reports (as needed) • Incident Response Plan	OpDiv-Specified	
6 – Other IT Procurements (Non-Commercial and Open Source Computer Software Procurements)	• Computer software, including the source code.	Prior to performing any work on behalf of HHS	

Attachment 2. Contractor Non-Disclosure Agreement

This NDA is to be completed by a contractor upon award of contract.
This is a baseline template and the OpDiv may modify the NDA to accommodate additional agency/contract requirements.

Information Technology Systems Security Contractor Non-Disclosure Agreement

Access to sensitive information (such as personally identifiable information [PII]), non-public information, confidential information, and/or Controlled Unclassified Information (CUI) from the files of the Department of Health and Human Services (HHS) is required in the performance of my official duties, under contract number between (HHS I/C Name or Component)_____ _____and my employer (Employer's Name) _____. I agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with relevant federal laws, regulations, and guidelines. *[OpDiv, insert applicable laws if any.]*

I affirm that I have received a written and/or verbal briefing by my company concerning my responsibilities under this agreement. I understand that violation of this agreement may subject me to criminal and civil penalties.

Signed: _____

Type or Print Name: _____

Date: _____

Witnessed by: _____

Date: _____

Copies are to be retained by:

HHS Contracting Officer Representative
Contractor's Contract Management
Individual Signatory