

ORDER FOR SUPPLIES AND SERVICES				IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution		PAGE 1 OF 1 PAGE(S)	
1. DATE OF ORDER 07/10/2020		2. ORDER NUMBER 47QPCA20F0019		3. CONTRACT NUMBER 47QTCA18D003V		4. ACT NUMBER A21937110	
FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 285F	ORG CODE Q00XF000	B/A CODE DS11	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE AF151	C/E CODE H04	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT	AI	LC	DISCOUNT	
7. TO: CONTRACTOR (Name, address and zip code) Shubhi Mishra THOUGHT OBJECT LLC 11710 PLAZA AMERICA DR STE 2000 RESTON, VA 20190-4743 United States 859-392-0425					8. TYPE OF ORDER B. DELIVERY		REFERENCE YOUR
					Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated. This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.		
9A. EMPLOYER'S IDENTIFICATION NUMBER 462689810		9B. CHECK, IF APPROP WITHHOLD 20%		Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.			
10A. CLASSIFICATION Woman Owned Business				10B. TYPE OF BUSINESS ORGANIZATION C. Corporation			
11. ISSUING OFFICE (Address, zip code, and telephone no.) Brian T Burns 10 CAUSEWAY ST BOSTON, MA 02222-1048 United States (617) 378-7565		12. REMITTANCE ADDRESS (MANDATORY) THOUGHT OBJECT LLC 11710 PLAZA AMERICA DR STE 2000 RESTON, VA 20190-0000 United States		13. SHIP TO (Consignee address, zip code and telephone no.) Dvora Wilensky 370 LENFANT PROMENADE, SW 8TH Floor West, Aerospace Bldg. Washington, DC 20447 United States 202-205-4997			
14. PLACE OF INSPECTION AND ACCEPTANCE Dvora Wilensky 370 LENFANT PROMENADE, SW 8TH Floor West, Aerospace Bldg. Washington, DC 20447 United States				15. REQUISITION OFFICE (Name, symbol and telephone no.) Rebecca E Refoy-Sidibe GSA Region 23 1800 F ST NW WASHINGTON, DC 20405-0001 United States (202) 809-4519			
16. F.O.B. POINT Destination		17. GOVERNMENT B/L NO.		18. DELIVERY F.O.B. POINT ON OR BEFORE 07/12/2021		19. PAYMENT/DISCOUNT TERMS NET 30 DAYS / 1.000 % 15 DAYS / 0.00 % 0 DAYS	
20. SCHEDULE							
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)		
0001	Facilitator	1	lot	\$208,216.70	\$208,216.70		
0002	Technical Lead	1	lot	\$247,120.90	\$247,120.90		
0003	Design Lead	1	lot	\$187,982.59	\$187,982.59		
0004	UX Researcher	1	lot	\$173,870.40	\$173,870.40		
0005	Backend Web Developer	1	lot	\$212,861.38	\$212,861.38		

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0006	Frontend Web Developer	1	lot	\$201,487.10	\$201,487.10
0007	Content Strategist	1	lot	\$66,597.12	\$66,597.12
0008	Visual Designer	1	lot	\$47,428.08	\$47,428.08
0009	Travel / ODCs	1	lot	\$14,500.00	\$14,500.00

21. RECEIVING OFFICE (Name, symbol and telephone no.) HHS/ACF, (202) 205-5842		TOTAL From 300-A(s)	
22. SHIPPING POINT Specified in QUOTE	23. GROSS SHIP WT.	GRAND TOTAL	\$1,360,064.27
24. MAIL INVOICE TO: (Include zip code) General Services Administration (FUND) The contractor shall follow these Invoice Submission Instructions . The contractor shall submit invoices electronically by logging into the ASSIST portal (https://portal.fas.gsa.gov), navigating to the appropriate order, and creating the invoice for that order. For additional assistance contact the ASSIST Helpdesk at 877-472-4877. Do NOT submit any invoices directly to the GSA Finance Center (neither by mail nor via electronic submission).	25A. FOR INQUIRIES REGARDING PAYMENT CONTACT: GSA Finance Customer Support	25B. TELEPHONE NO. 816-926-7287	
	26A. NAME OF CONTRACTING/ORDERING OFFICER(Type) Brian T Burns	26B. TELEPHONE NO. (617) 378-7565	
	26C. SIGNATURE Brian T Burns 07/10/2020		
GENERAL SERVICES ADMINISTRATION	1. PAYING OFFICE	GSA FORM 300 (REV. 2-93)	

General Services Administration
Federal Acquisition Service
Technology Transformation Services
18F and Office of Acquisition
[1800 F Street NW | Washington, DC | 20405](#)

TANF Data Reporting System (TDRS) Software Development Services

Performance Work Statement

1.0 Background and Purpose

1.1 Purpose

In fiscal year 2020, the [Office of Family Assistance](#) (OFA) within the Administration for Children and Families (ACF) entered into an interagency agreement with [18F](#) within the Technology Transformation Services (TTS) to provide assisted acquisition services for the procurement of software development services in support of the Temporary Assistance for Needy Families (TANF) program. OFA is seeking a contractor to assist with the development of a new TANF Data Reporting System (TDRS). 18F will award the contract and provide contractual and administrative support to OFA. OFA will oversee contractor performance and review deliverables. 18F will provide procurement and technical support to OFA for the life of the contract.

1.2 Background

18F applies modern methodologies and technologies to improve the public's experience with government by helping agencies make their services more accessible, efficient, effective, and by providing services that exemplify these values.

The Office of Family Assistance (OFA) has entered into an interagency agreement (IAA) with 18F for assisted acquisition services. 18F will acquire the services requested in this solicitation on behalf of OFA and administer the contract in post award.

OFA, within the Administration for Children and Families (ACF), administers the Temporary Assistance for Needy Families (TANF) program on behalf of the Department of Health and Human Services (HHS). Since 1996, the TANF program has served as one of the nation's primary economic security and stability programs for low-income families with children. TANF is a block grant that provides \$16.6 billion annually to states, territories, the District of Columbia, and federally-recognized Indian tribes. These TANF jurisdictions use federal TANF funds to provide income support as well as a wide range of services to vulnerable families with minor children.

As part of oversight and administration of the TANF Program, OFA operates the TANF Data Reporting System (TDRS).

OFA's TANF grantees submit data to TDRS that they are legislatively-mandated to report. OFA then aggregates the data and uses it for descriptive analyses and program accountability, most notably through the work participation rate calculations. Work participation rates measure the degree to which families receiving TANF assistance are engaged in work activities specified under federal law. States, territories, and tribes must meet both an overall work participation rate and a two-parent work participation rate or be subject to a financial penalty.

The existing system was developed in the late 1990s with only minor updates in the past 20 years.

The TANF grantees usually generate their data in one of the following ways (review [information about the incoming data format](#)):

- Using a legacy tool (ftanf.exe) that exports files in a special text format
- Using their own software to export the data
- Emailing their data to an OFA staff member to be entered for them

The data is then uploaded using secure file transfer protocol (SFTP) into a system which then periodically attempts to process the data and import it into the database OFA staff uses for analysis. OFA staff access the data via direct read-only SQL queries using tools like python, Jupyter Notebooks, and SAS.

The database currently is around 50GB in size, though most of it is historical data which will not need to be migrated. Most of the tables contain between 700,000 to 1,300,000 rows and most of the data is stored in seven tables. These tables are renamed periodically so there is a historical record. Access to this data is extremely

limited, both because the data is sensitive (contains personally identifiable information or PII) and because managing access to these aging systems is difficult.

2.0 Scope

OFA seeks agile software development services to begin work toward the product vision of a user-friendly data system. The services to be provided under this task order will include all aspects of the software development process — including initial planning, design, user research, software development and coding, prototyping, documentation, testing, and configuration. And once the new app is released, the contractor will assist with troubleshooting, bug resolution, operational support, and incident response.

OFA is not looking to migrate data from the existing TANF system to the new system. OFA will continue to access the old database independently for any longitudinal reporting. They are prepared to adapt their current tools to whatever new table structure is created with the new system. However, there will probably be a transition period where data uploaded to the old system with sftp will need to be synced to the new system, and vice versa, but this is the only legacy integration required. The transition from the legacy system to the new system will be a partnership between the ACF OCIO and the contractor. Historical data is not needed in the new system because longitudinal analyses are done outside the system and we already have that data to combine with new data.

Data validation rules will need to be adapted from current data validation rules (see ACF-199 Instructions and Error Codes). The contractor is expected to continue user research and conversations with OFA to develop the updated validation rules.

<https://www.acf.hhs.gov/ofa/resource/tanf-acf-pi-2017-05>

<https://www.acf.hhs.gov/ofa/resource/tanfedit/index>

<https://www.acf.hhs.gov/ofa/resource/tribal-tanf-data-coding-instructions>

2.1 Performance objectives

2.1.1 PWS Objectives/Quality Assurance Surveillance Plan (QASP)

Deliverable 1	Accepted Features
Performance	At the beginning of each sprint, the Product Owner and

Standard(s)	development team will collaborate to define a set of user stories to be completed during the sprint. Acceptance criteria for each story will also be defined. The development team will deliver code and functionality to satisfy these user stories.
Acceptable Quality Level	Delivered code meets the acceptance criteria for each user story. Incomplete stories will be assessed and considered for inclusion in the next sprint.
Method of Assessment	Manual review
Due Date	Every sprint

Deliverable 2	Tested Code
Performance Standard(s)	Code delivered under the order must have substantial test code coverage. Version-controlled HHS GitHub repository of code that comprises products that will remain in the government domain.
Acceptable Quality Level	Minimum of 90% test coverage of all code. All areas of code are meaningfully tested.
Method of Assessment	Combination of manual review and automated testing
Due Date	Every sprint

Deliverable 3	Properly Styled Code
Performance Standard(s)	<u>GSA 18F Front- End Guide</u>
Acceptable Quality Level	0 linting errors and 0 warnings

Method of Assessment	Combination of manual review and automated testing
Due Date	Every sprint

Deliverable 4	Accessible
Performance Standard(s)	Web Content Accessibility Guidelines 2.1 AA standards
Acceptable Quality Level	0 errors reported using an automated scanner and 0 errors reported in manual testing
Method of Assessment	Combined approach using automated and manual testing with tools equivalent to Accessibility Insights and/or the DHS Trusted Tester process .
Due Date	Every sprint

Deliverable 5	Deployed
Performance Standard(s)	Code must successfully build and deploy into the staging environment.
Acceptable Quality Level	Successful build with a single command
Method of Assessment	Combination of manual review and automated testing
Due Date	Every sprint

Deliverable 6	Documented
----------------------	-------------------

Performance Standard(s)	Summary of user stories completed every two weeks. All dependencies are listed and the licenses are documented. Major functionality in the software/source code is documented, including system diagram. Individual methods are documented inline in a format that permits the use of tools such as JSDoc. All non-inherited 800-53 system security controls are documented in the Open Control or OSCAL format and HHS Section 508 Product Assessment Template (PAT) are updated as appropriate.
Acceptable Quality Level	Combination of manual review and automated testing, if available
Method of Assessment	Manual review
Due Date	Every sprint

Deliverable 7	Secure
Performance Standard(s)	Open Web Application Security Project (OWASP) Application Security Verification Standard 3.0
Acceptable Quality Level	Code submitted must be free of medium- and high-level static and dynamic security vulnerabilities
Method of Assessment	Clean tests from a static testing SaaS (such as Snyk or npm audit) and from OWASP ZAP, along with documentation explaining any false positives
Due Date	Every sprint

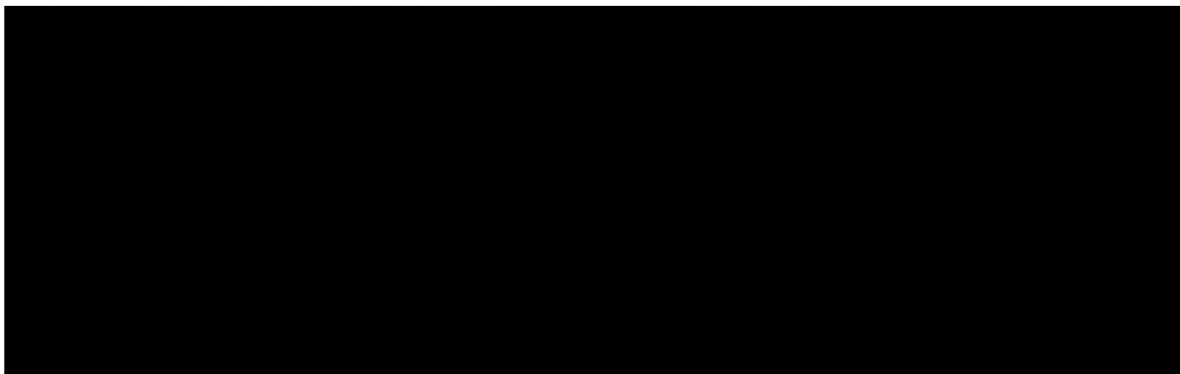
Deliverable 8	User research
----------------------	----------------------

Performance Standard(s)	Usability testing and other user research methods must be conducted at regular intervals throughout the development process (not just at the beginning or end).
Acceptable Quality Level	Research plans and artifacts from usability testing and/or other research methods with end users are available at the end of every applicable sprint, in accordance with the contractor's research plan.
Method of Assessment	OFA will manually evaluate the artifacts based on a research plan provided by the contractor at the end of the second sprint and every applicable sprint thereafter.
Due Date	As needed

2.1.2 Technical approach

Who we are and why will we succeed

We are passionate about creating public-facing digital products that are meaningful and accessible. As agile evangelists, we firmly believe in continuously testing our assumptions and iteratively building impactful products in the most transparent, collaborative, and responsive way possible. Furthermore, we have the valuable

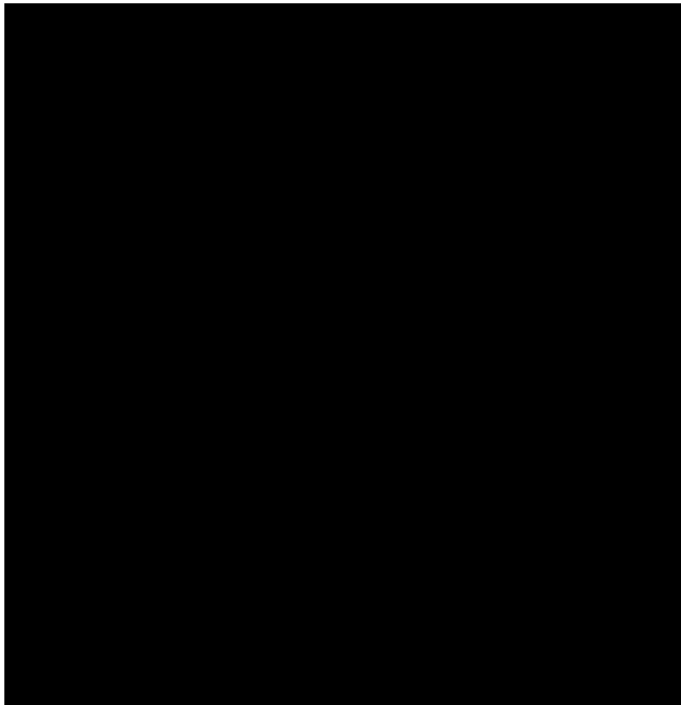


experience of having delivered projects immensely similar to the TANF Data Reporting System (TDRS): the [Home Mortgage Disclosure Act \(HMDA\) Platform](#) and [Data Browser](#) for the Consumer Financial Protection Bureau (CFPB) in the [open source](#). Raft used a human-centered design approach to transform a legacy application into the web-based HMDA Platform ([link to transformation video](#)) used by 10,000 financial

institutions with over 20,000 annual data submissions. Raft also transformed the outdated HMDA explorer used to download datasets into the HMDA Data Browser. Both applications are running in production and continuously improved upon, and CFPB has been delighted with the results. From our experience with HMDA, we understand the engineering and user research complexities involved in TDRS, how to address the pain points of TDRS, and will be able greatly reduce the time required for the development and production rollout of the application.

How we will manage TDRS

We will hold a kickoff workshop with the Product Owner (PO) and key stakeholders to: (1) confirm the overall product vision, identify limitations, and define the criteria for measuring product success; (2) break down the vision into phases, define the goal of the minimum viable product (MVP), and group existing user stories into these phases; and (3) demonstrate HMDA applications as ‘prototypes’ to learn what features, user flow, concepts, and messaging resonate with the stakeholders. As shown in Figure 1: Product Roadmap Diagram, one of the outcomes of the workshop will be a product roadmap that will break down the overall vision of TDRS into phases (e.g., TANF uploader, TANF validator, etc.). Each phase will be defined by outcome-based goal(s)



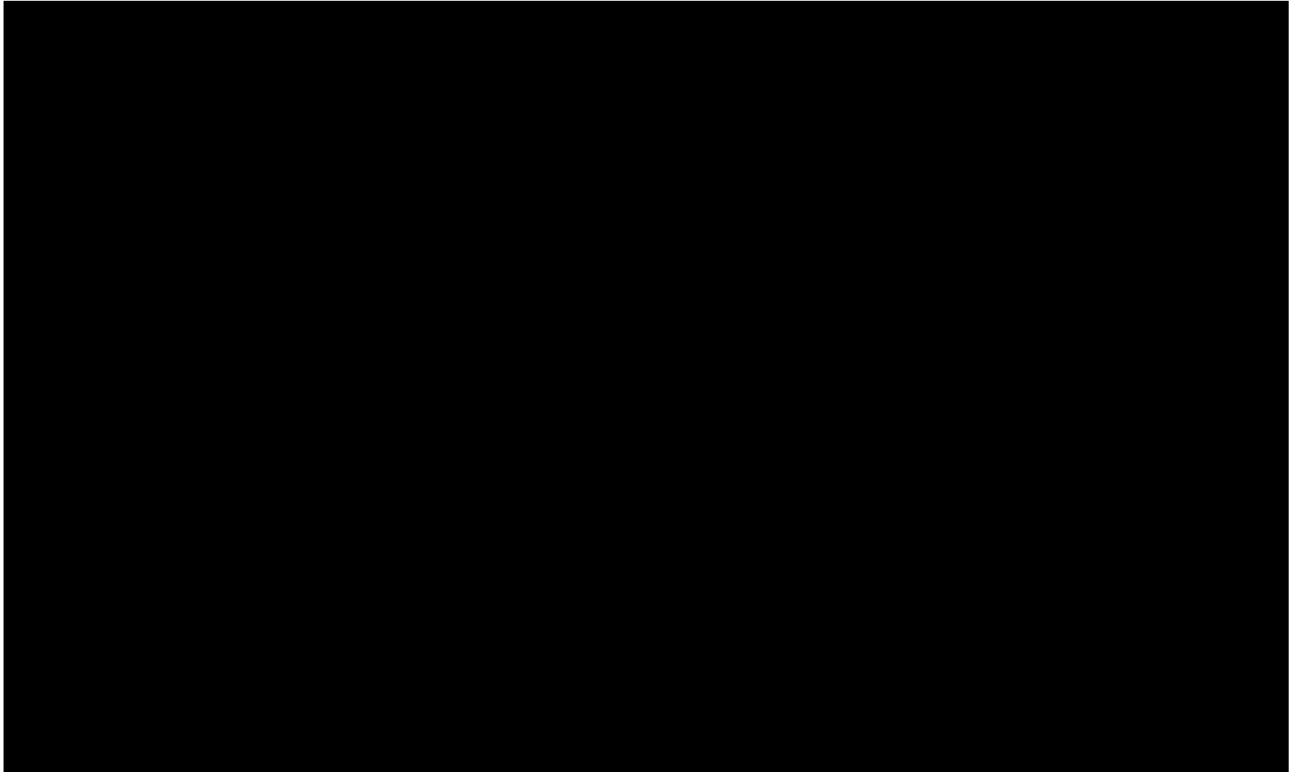
(e.g., use app to make data upload easier), the value it delivers to TDRS user type (e.g., grantees have a *better* way to upload TANF transmission files all at once), measured by defined key performance indicators (KPIs) around adoption, utilization, retention, submission, review response times, etc., (e.g., adoption - number of grantees using the app to upload), and have a completion timeline. We will use the KPIs to continuously measure post launch success (e.g., number of grantees using the app to complete a submission the following quarter, number of attempts/iterations it took submit data after failed validation, number of help desk tickets received to

confirm data submission, data processing time, etc.) and propose refinements and improvements. Each outcome-based goal will identify specific functionalities or ‘themes’ (e.g., grantee-level user research, data modeling, etc.) that need to be

implemented to meet the goal. The themes will either be broken into new user stories or formed from existing TDRS user stories. These themes will be defined during milestone planning that will happen every six weeks (~ three sprints), issues will be assigned to three upcoming sprint cycles to achieve the themes. The milestone planning will be relative and will enable us to track and evaluate progress to guide future planning. The issues assigned to specific sprints will be discussed during sprint planning that will happen every two weeks. We will use modified Fibonacci scale – 1, 3, 5, etc., to estimate story points. Each team member will vote with a point, discuss estimation, and PO will select user stories based on the discussion (~not to exceed 8/13 on the scale). We will use *completed* story points to calculate velocity after each sprint. The baseline velocity will be rounded average of the *completed* story points for the first 3 sprints – i.e., rounded value = sum of story points for first **three** sprints / **three**. At the end of each sprint, we will hold review session to demonstrate progress and retrospective to discuss what worked well and what could be improved. We will hold daily scrums to resolve any blockers and ensure team coordination and each week share a summary of what we shipped. We will standardize our workflow and processes by defining template for issues and pull requests (PR), issue hand off process, and definition of done (DoD). The issue template will include a clear description with an acceptance criteria (AC) checklist and DoD, such as: (1) Product (AC have been met); (2) Design (usability has been validated, etc.); (3) Dev (code has been reviewed, etc.). For the blocked issues, we will note the dependency, tag the other issues, and label them blocked. For issues that grow in scope, we will create and link the parent issue to the child issue and label it as an Epic or a Future Enhancement. Furthermore, we will work in our (Raft) branch of the TANF-app fork and open PRs to merge into the dev branch of TANF-app. We will review the deployed application in the Cloud.gov dev environment and open a PR from dev to staging for review by 18F and OFA. All PRs opened by our team will include summarized list of issues/user stories implemented in the sprint, screenshots/GIFs of functionality, successful automated end-to-end testing, accessibility compliance, and vulnerability scanning. Using our approach, we will deliver the deliverables per the QASP.

How we will continue user research

We will also hold alignment workshops with PO and 18F to review the completed user research, create core UX principles (e.g., design principles, user personas, content and style guide, journey map) and establish design patterns from USDWS, if not done so already. Based on the identified gaps and findings from the workshops, our team will initiate design or user research cycles as shown in Figure 2.



The core UX principles and design patterns will guide creation of mockups or prototypes that will be tested via usability testing sessions typically scheduled for 60 minutes with the recruited users. The user research and usability testing plans will state learning objectives, assumptions and hypotheses to test, list interview methods (e.g., contextual, task based etc.) and demographics, conversation guide, logistics, research timeline, and the expected outcomes. We will do in-person user research at the locations of the participants, and for remote user research we will use lookback.io or similar tools, if available via 18F/OFA. The feedback from these user interviews will be collaboratively synthesized as user and product needs for prototyping and development, and opportunities for improvement, all of which will be added to the backlog as issues/user stories. This overall research process will iteratively continue until all backlog items have been addressed. We will also frequently hold realignment workshops and may hold design studios to sketch out any confusing or hard elements. We will also hold data workshops to do a detailed walkthrough of TANF and SSP-MOE transmission file layouts (T1-T7) and FTANF spreadsheet to map out how each data field, data edit (fatal/warning), edit description, data length etc., will be structured into backend classes, domain models, database tables, and APIs.

How we will develop TDRS

Our proposed event-driven architecture is a loosely coupled modular design that is cloud vendor agnostic, scalable, supportable, leverages open-source libraries and is inspired from [successful delivery of HMDA applications](#). We will be re-using parts of

the open source code and architecture from HMDA application to accelerate our development and shorten the time to production. We will additionally leverage the CI/CD, FTANF, and transmission file layout mapping related work done in the TANF-app prototype built by 18F.

Backend: We will use a strongly-typed language such as Java or Python with SpringBoot and Django frameworks respectively. Using a strongly-typed language will: (1) prevent errors in code by bounding variables to specific object maps of the TANF & SSP-MOE transmission file layouts; (2) keep the code maintainable by using enumeration (*enum*) to represent a set of numbered values mapped to plain language (e.g., as per fatal edit T2-017 “family affiliation” in section T2 is assigned a number between 1 to 5, where “1” is member of an eligible family receiving assistance, and “2” is parent of a minor child, etc.); (3) enable concurrent/non-blocking I/O leading to high scalability at low cost; and (4) be easily supported by [18F](#) and [HHS](#). We will also use ubiquitous Domain Specific Language (DSL) to incorporate the edit validation logic into code as plain English (e.g., [data edit written for HMDA in this language](#)) so the non-developers can easily read and propose updates.

Frontend: We will use ReactJS and the [create-react-app](#) framework with major libraries such as React Router for client-side page routing, Redux for application state management, and Reselect to memorize state selectors. We will also employ [USWDS](#) and [Sass](#) to build styles, and [Webpack](#) to bundle the app into a deployable deliverable with a small footprint. Unit testing of components will be done using Jest with Enzyme and cross browser testing will include Internet Explorer. We will store documentation in markdown on GitHub, load it on-demand with the [Fetch API](#), and render it dynamically using [markdown-to-jsx](#). This will enable documentation updates on the TANF app via PRs in GitHub rather than needing deployments (e.g. [HMDA Docs](#)).

Database & PII: We will use PostgreSQL via the Cloud.gov AWS RDS service broker. All information would be stored in a single database that will include table layout derived from the data workshop held to discuss the TANF and SSE MOE transmission files. To increase efficiency of SQL queries, we will create materialized views that will be automatically refreshed, create optimized multi column indices on each table, and regularly vacuum tables to reclaim storage occupied by dead tuples. Data fields containing PII (e.g., SSN in T1 item 33, 69 and T2 item 16) will be stored using [PGP](#) encryption via [pgcrypto](#). The public key will be used to encrypt and private key to decrypt the data.

API: We will use RESTful APIs to enable easier integration with external applications. APIs will allow multiple *uploads* but only allow *submission* of validated data. APIs will enable grantee admins to authenticate (via Login.gov), upload, validate, view fatal and warning edit errors in plain language, append metadata, and submit the data. It will

also allow OFA analysts and program directors to customize validations, download reports in multiple formats, and view characteristics of cases and caseload trends overtime. APIs will validate the data in real-time and leverage web-sockets to provide constant progress updates (e.g., row number) of the flat file being validated. We will document the APIs with [OpenAPI](#), use [slate](#) to render the API documentation, and deploy using [gh-pages](#) (e.g. [HMDA API doc](#)).

Authentication: We will implement authentication via Login.gov using OpenID Connect (OIDC) and parse the ID and access token to extract user login details, verify the digital sign, validate the audience parameter, and assign roles and responsibilities for different user types.

Accessibility and Linting: We will use [WAVE](#) and manual testing via keyboard navigation to scan the application pages for accessibility compliance with [HHS Section 508](#) and regularly update the Product Assessment Template (PAT) . For linting, we will use [eslint](#) to analyze JavaScript files and find patterns in code that do not adhere to the defined style rules that are based on [Airbnb's style guide](#) and [Prettier](#).

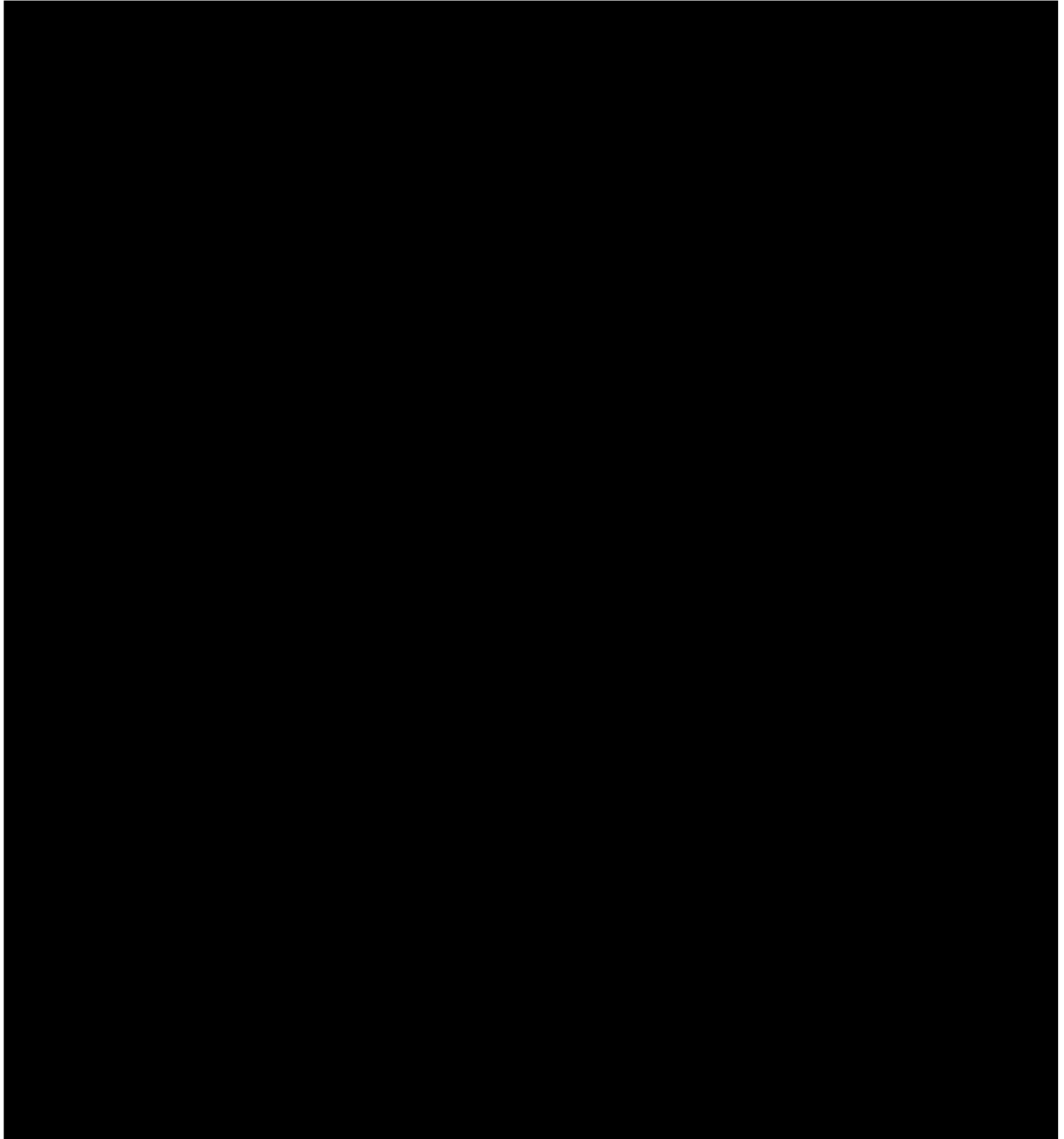
Automated Testing and Security: We will use CircleCI code coverage metrics to remain above 90% as per QASP. We will go the extra step by building upon TANF-app CircleCI pipeline by integrating end-to-end testing using [Cypress](#) and [Newman](#), accessibility using [Pa11y](#), container vulnerability scanning using [Trivy](#), and static code scanning using [Snyk](#). These integrations will enable automated scans on each PR. Any PR with a failed scan will not be merged until the issues are resolved. To remain cloud vendor agnostic, in addition to continue using docker containers to deploy, we will also configure secrets, object store keys, host URLs, etc., to be securely provisioned using environment variables at container runtime.

Technical Debt Management: Our technical debt management strategy is built upon having a sustainable architecture and test coverage enabling our team to refactor code with high confidence. We will ensure that no single class is too long, Don't Repeat Yourself (DRY) principle is used, documentation is continuously improved, code maintainability is enabled via CircleCI, and [Dependabot](#) is used to open automated PRs to keep the dependencies up-to-date.

On-boarding users to new system: We will work with ACF OCIO to prepare a strategy to transition states, tribes, and territories (STTs) from using the legacy system to the new system. Having done this successfully in the past with the HMDA Platform by transitioning 10k+ financial institutions from legacy system, we're well aware of the challenges and strategies that can be employed such as ensuring STTs are enrolled into Login.gov, [creating onboarding videos](#), conducting webinars, and a user experience that motivates STTs to use the new system.

How we will resolve obstacles

Leveraging lessons learned from our HMDA experience, we have curated a list of obstacles that may arise during TDRS development and our proposed solutions.



2.2 Operating constraints

2.2.1 System Requirements

The System must:

- Incorporate an intuitive, web-based interface that is accessible from both internal and external platforms, including desktops, laptops, tablets, thin/zero clients, and mobile devices
- Incorporate application programming interfaces (APIs) to intermediate major components
- Be highly available to users and have adequate capacity to handle the load
- Include Login.gov user authentication and authorization functionality and use open source encryption protocols for all data transmission.
- Be developed in Cloud.gov and must eventually migrate to another ACF cloud environment. The type of environment is unknown at this time, so the application should be written to be as operationally portable as possible.

2.2.2 Authentication Requirements

The software must have multi-factor authentication for the grantees and PIV authorization for the OFA staff and key personnel. The Login.gov system has already been procured to fulfill this requirement.

2.2.3 Software Requirements

The software architecture must be extensible to allow for future development including the addition of new statutorily mandated data reporting. The code base must incorporate analytics, monitoring, testing, and measurement tools. Application design and development must use plain language to the extent practical.

2.2.4 Design Requirements

Any website that is developed or otherwise delivered as a result of this contract shall be in compliance with the [website standards](#) of the Technology Transformation Services of the General Services Administration.

The contractor will employ the U.S. Web Design System (USWDS) and create design elements that are reusable by OFA.

2.2.5 Environments

The System will be developed and initially hosted on Cloud.gov (a FedRAMP-certified internet-connected Platform as a Service). OFA will own and manage the Cloud.gov account and create development, staging, and production environments for this project within that account. The contractor will have access to the development environment and will be responsible for maintaining that environment. The contractor must post all developed code to the public source repository as designated by OFA. OFA will be responsible for creating and managing this repository. OFA will be responsible for setting up and maintaining a Continuous Integration/Continuous Deployment system to automate the deployment of the code in GitHub, and the contractor will be able to contribute configuration-related code that will improve it as needed-related code that will improve it as needed. OFA will be responsible for creating, maintaining, and managing the Login.gov integrations.

2.2.6 System Access

All contractor personnel working under the resulting contract will need to obtain a Homeland Security Presidential Directive 12 ([HSPD-12](#)) low risk security clearance (or moderate risk security clearance if handling PII).

In addition, the contractor's key personnel will need to obtain a personal identity verification (PIV) card in order to perform legacy system integration work. See Appendix 1 - Section 1.6 for details.

Contractor personnel that are required to obtain a PIV card will be issued a government-furnished laptop from HHS/ACF. Any work that requires access to and handling of PII must be performed on the HHS/ACF government-furnished laptop. Contractor personnel that are not required to obtain a PIV card can use contractor-furnished equipment to perform work. The government does not anticipate that contractor personnel will need to access PII data initially.

Contractors may have to establish multi-factor authentication (MFA) to access systems that require government laptops with PIV cards or to access other applications that require MFA.

3.0 Contractor roles and responsibilities

3.1 Roles and responsibilities

The contractor must designate a Facilitator, Technical Lead, and Design Lead as Key Personnel for this project.

The Facilitator will be a direct liaison to the Government product team, and will be responsible for the supervision and management of all of the Contractor's personnel.

The Technical Lead must have a full understanding of the technical approach to be used by the Contractor's team and will be responsible for ensuring that the Contractor's team follows that approach.

The Design Lead must have a full understanding of the research approach and design patterns to be used by the contractor's development team and will be responsible for ensuring that the contractor's development team follows that approach.

Key Personnel substitutions must be approved by the Government in writing, and will only be justified by the Government request, sudden illness, death, change of employment, or termination of employment for cause. Contractor requests for a substitution of Key Personnel must include a detailed explanation of the justifying circumstances, and a complete résumé for the proposed substitute or addition, including skills, experience, education, training, and security level. The Government's failure to approve a proposed substitution will not constitute grounds for non-performance by the Contractor, or form a valid basis for any claim for money or any equitable adjustment.

4.0 Government roles and responsibilities

4.1 Makeup of team

The Government team consists of the CO, the GSA Contracting Officer's Representative (COR), the OFA Contracting Officer's Representative (COR), and a Product Owner (PO).

4.2 Contracting personnel

4.2.1 Contracting Officer

The CO for this buy is identified on the cover page. Questions, comments, issues, or responses must be submitted through the methods outlined in the solicitation. Any other forms of communication will not be considered. After award, the CO will delegate most of the day-to-day tasks to the OFA COR and PO.

4.2.2 Other members

A delegation letter for both CORs will be provided to the awardee, outlining the contractual roles and responsibilities of the CORs. The roles and responsibilities of the PO will be provided no later than the kickoff meeting that will follow awarding the task order. The names and email addresses of the entire team will also be provided no later than the kickoff meeting as well.

5.0 Terms and conditions

5.1 Travel and other direct costs (ODC)

Occasional travel is anticipated. The OFA COR will notify the contractor via email when travel is anticipated. Actual travel costs to government facilities will be reimbursed in accordance with federal travel regulation ([FTR](#)). No travel will be reimbursed if travel to/from off-site meetings is less than 60 miles.

Other direct costs (other than travel) are permitted and can be added to this task order with written consent of the CO.

5.2 Period and place of performance

The period of performance will include a one-year base period starting on July 13, 2020 with two one-year option periods. The contract type for this effort will be time and materials (T&M).

Normal working hours are from 9:00AM to 5:00PM Eastern time Monday through Friday. The contractor will generally be expected to be readily available during core working hours from 10:00am to 4:00pm Eastern time Monday through Friday. They are not expected to work federal holidays. If the federal government shuts down for any reason, contractors may seek approval from the COR to telework during this time.

The contractor may choose the location(s) from which to perform the required software development services. The contractor will not be required to work at a government facility however, occasional travel to government facilities may be required. Actual travel costs to government facilities will be reimbursed in accordance with [federal travel regulation](#). All travel must be approved by the contracting officer's representative (COR) prior to booking.

5.3 Payment and invoicing procedures

5.3.1 Invoicing Schedule

The contractor may invoice once services or products for the awarded type and quantity of the order have been delivered, inspected (which includes, but is not limited to, confirming that the services were rendered and/or product(s) were delivered and functioning properly, and are accessible and usable by the teams using the product), and accepted by written confirmation of the COR through the CO. Acceptance will occur electronically via GSA's electronic web-based order processing system, currently ASSIST, by accepting the invoice generated by the contractor. Electronic acceptance of the invoice by the COR is considered concurrence and acceptance of services.

The contractor must submit a final invoice within 60 calendar days from government acceptance. No further charges are to be billed following the final invoice submission. A completed and signed Release of Claims ([GSA Form 1142](#)) shall be uploaded to the ASSIST with the submission of a final invoice.

5.3.2 Content of Invoice

In addition to the items below, the contractor shall submit proper invoices as specified in FAR 52.212-4(g):

- GSA Order Number
- Order ACT Number
- QP Number (funding document number)
- Prompt Payment Discount
- Remittance Address
- POP for Billing Period
- POC and Phone Number
- Invoice Amount
- Final Invoice Marked as “Final”
- Name of Product, Quantity of Product, and Part Number of Product matching award documents.

In addition to the requirements for a proper invoice specified in FAR 52.212-4 (g), invoices must include the Prompt Payment clause, FAR 52.212-4(i)(2) and Payments under Time and Materials and Labor Hours Contracts, FAR 52.232-7.

5.3.3 Invoice Submission

The contractor shall submit invoices electronically by logging into the [ASSIST portal](#), navigating to the appropriate order, and creating the invoice for that order. This is the only acceptable means for invoice submissions.

No paper invoices shall be accepted. For additional assistance, contact the ASSIST Helpdesk at 877-472-4877 or via email at assist.servicedesk@gsa.gov.

5.3.4 Limitation of Funds

The contractor shall notify the CO in writing when it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the contract by the government or, (2) if this is a cost-sharing contract, the amount

then allotted to the contract by the government plus the contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the contract.

Sixty days before the end of the period specified in the contract, the contractor shall notify the CO in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract or for any further period specified in the contract or otherwise agreed upon, and when the funds will be required.

General Services Administration
Federal Acquisition Service
Technology Transformation Services
18F and Office of Acquisition
[1800 F Street NW | Washington, DC | 20405](#)

TANF Data Reporting System (TDRS) Software Development Services

Appendix 1

Contract Terms and Conditions

1.0 Transparency Policy & Security Requirements

Contractors are advised that TTS reserves the right to publish documents associated with this requirement on a publicly-available website, including any Requests for Quotation (including amendments), Question and Answer exchanges with contractors (source-identifying information removed), and other relevant information that is not confidential or proprietary in nature or source selection sensitive information that would otherwise implicate procurement integrity concerns.

Upon award, TTS may publish the total awarded price and certain non-source-identifying data (for example, the number of bids, the mean price, median, and standard deviation of price). During the performance of this task order, TTS may similarly publish data related to project management (for example, user stories, milestones, and performance metrics) and top-line spending data.

1.1. Section 508 Compliance

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

A. Section 508 of the Rehabilitation Act of 1973

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

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

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

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

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

Section 255 address the telecommunications products covered including wired and wireless telecommunication devices such as:

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

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

B. Functional Performance Criteria

Section 1194.31 Functional Performance Criteria

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

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards#subpart_c

C. FAR Part 39 - Acquisition of Information Technology

a. 39.000 -- Scope of Part.

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

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

(b) Information and information technology.

b. 39.001 -- Applicability.

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

c. 39.002 -- Definitions.

As used in this part--

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

d. 39.104 – Information Technology Services.

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

(a) Cannot be met without that requirement; or

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

e. 39.106 -- Contract Clause.

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

f. 39.201 Scope of subpart.

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

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

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

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

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

g. 39.202 Definition.

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

h. 39.203 Applicability.

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

(b)

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

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

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

(c)

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

(2) The requiring official must document in writing the no availability, including a description of market research performed

and which standards cannot be met, and provide documentation to the contracting officer for inclusion in the contract file.

i. 39.204 Exceptions.

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

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

(b) Is for a national security system;

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

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

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

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

(i) The difficulty or expense of compliance; and

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

(2) *Documentation.*

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

(ii) When acquiring commercial items, an undue burden determination is not required to address individual standards that cannot be met with supplies or service available in the commercial marketplace in time to meet the agency delivery requirements (see 39.203(c)(2) regarding documentation of nonavailability).

<http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm>

j. 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.

k. Installation, Configuration & Integration Services

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

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

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

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

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

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

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

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

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

D. Revised 508 Standards, Safe Harbor and FAR Update

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

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

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.”

E. Contract Staff and Vendors

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

- (a) In order to facilitate the Government’s determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offeror must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offeror or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy. (See HHS PAT Link below.

To determine whether proposed EIT services meet applicable Section 508 accessibility standards, offeror must provide enough information to assist

the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

- (a) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS website: (<http://www.hhs.gov/web/508>). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
- (b) The leaderboard below demonstrates how compliant our websites are with Section 508. The accessibility of websites for each Operating Division is determined each month by an automated scan of every page of every website.
- (c) Scores: Acceptable- 76% and above. Needs Improvement- 75.99% and below.
- (d) Deliverables: 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

1.2. Privacy Act

Performance of this Task Order may require that personnel have access to privacy information. Contractor personnel shall adhere to the privacy act, Title 5 of the U.S. Code, Section 552a and any other applicable applicable rules and regulations.

1.3. Protection of Information

The Contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this Task Order. The Contractor shall also protect all Government data by treating information as sensitive. All information gathered or created under this Task Order shall be considered as Sensitive but Unclassified (SBU) information. The use of this data is subject to the privacy act and shall be utilized in full accordance with all rules of conduct as applicable to privacy act Information.

1.4. Organizational Conflicts of Interest

The prospective Contractor certifies, to the best of its knowledge and belief, that it is not aware of any information bearing on the existence of any potential organizational conflict of interest.

If the prospective Contractor cannot so certify, it shall provide a disclosure statement in its proposal which describes all relevant information concerning any past, present, or planned interests bearing on whether it (including its chief executives and directors, or any proposed consultant or subcontractor) may have a potential organizational conflict of interest.

Prospective Contractors should refer to FAR Subpart 9.5 and GSAM Part 509 for policies and procedures for avoiding, neutralizing, or mitigating organizational conflicts of interest.

If the Contracting Officer determines that a potential conflict exists, the prospective Contractor shall not receive an award unless the conflict can be avoided or otherwise resolved through the inclusion of a special contract clause or other appropriate means. The terms of any special clause are subject to negotiation.

1.5. Data Rights and Ownership of Deliverables

Data Rights and Ownership of Deliverables – OFA intends that all software and documentation delivered by the Contractor will be made publicly available without restriction. This software and documentation includes, but is not limited to, data, documents, graphics, code, plans, reports, schedules, schemas, metadata, architecture designs, and the like; all new open source software created by the Contractor and forks or branches of current open source software where the Contractor has made a modification; and all new tooling, scripting configuration management, infrastructure as code, or any other final changes or edits to successfully deploy or operate the software. Contractor's should not be using any pre-existing commercial code unless it is provided by the Government. For the avoidance of doubt, the foregoing is included in the definition of "data" set forth in the FAR clause at 52.227-17, incorporated into this contract.

To the extent that the Contractor seeks to incorporate into the software delivered under this task order any software that was not first produced in the performance of this task order, OFA encourages the Contractor to incorporate either software that is in the public domain, or free and open source software that qualifies under the Open Source Definition promulgated by the Open Source Initiative. In any event, the Contractor must promptly disclose to OFA in writing, and list in the documentation, any software incorporated in the delivered software that is subject to a license fee.

If software delivered by the Contractor incorporates software that is subject to an open source license that provides implementation guidance, then the Contractor must ensure compliance with that guidance. If software delivered by the Contractor incorporates software that is subject to an open source license that does not provide implementation guidance, then the Contractor must attach or include the terms of the license within the work itself, such as in code comments at the beginning of a file, or in a license file within a software repository.

The Government data rights of software deliverables and all other data first produced in the performance of this task order shall be in accordance with **FAR 52.227-17 Rights in Data -- Special Works**. The Government may require the contractor to assign its copyright in such data to the Government in accordance with **FAR 52.227-17(c)(1)(ii)** or to publicly post it with an appropriate notice.

Ownership of code repositories furnished as Government-Furnished Information (GFI) and Government-provided data entered into any and all systems, system documentation, and other related system information shall reside with the Government.

1.6. Personnel Security Requirements

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;
- Federal Information Processing Standards Publication (FIPS PUB) Number 201,
- FAR Subpart 4.13,
- FAR 52.204-9, and
- HHS HSPD-12 policy

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

1.7. IT Security Requirements

A. Baseline Security Requirements

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

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

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

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

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

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

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

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

d. Comply with the Privacy Act requirements.

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 Categories, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the contractor shall work with the ACF security team to categorize information or information systems. The categorization can change at any time throughout the lifecycle of the system. The contractor shall ensure proper controls are implemented based on the categorization.

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

a. marked appropriately;

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

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

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

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

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

The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS and ACF policies. Unauthorized disclosure of information will be subject to the HHS/ACF sanction policies and/or governed by the following laws and regulations without limitation:

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

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

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

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

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

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

- a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
- b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.
- c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and ACF-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the contracting officer's representative (COR) prior to implementation of the solution.
- e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

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.

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.

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

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

B. Training

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

2) Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the COR) 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. A copy of the training records shall be provided to the CO and/or COR within 30 days after contract award and annually thereafter or upon request.

C. Rules of Behavior

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

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

D. Incident Response

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

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

- 1) Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident.
- 2) Notify affected individuals only as instructed by the Contracting Officer or designated representative.
- 3) Report all suspected and confirmed information security and privacy incidents and breaches to the ACF Incident Response Team (IRT), COR, CO, ACF SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic as defined in ACF's Incident Response Policy.
- 4) Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

E. Position Sensitivity Designations

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

Non-Sensitive High Risk Tier 4 SF 85P

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within 3 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 24 hours of the change. The COR will notify the

Contractor of the appropriate level of investigation required for each staff member. If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

F. Contract Initiation and Expiration

- 1) General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Solution Development Life Cycle (SDLC) processes, ACF Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the ACF SDLC framework and methodology.
- 2) System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-160 Volume 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, at a minimum, for system development.
- 3) Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
- 4) Notification. The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 48 hours before an employee stops working under this contract.
- 5) Contractor Responsibilities Upon Physical Completion of the Contract. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information

has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or ACF policies.

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

G. 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.

1.8. Records Management

A. Applicability

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

B. Definitions

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

- 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.

C. 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)

- a. Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
- b. Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.
- c. Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.
- d. Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

- e. Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.
- f. Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.
- g. Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

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 subcontractor) 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.

1. ACF owns the rights to all data and records produced as part of this contract. ACF shall have unlimited rights to use, dispose of, or disclose all data contained in any and all contract deliverables as it determines to be in the public interest and in accordance with the data rights clauses applicable to this contract

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.

1.9. Contractor Transition

Ensure and agree that all deliverables, products, licenses, designs, data, documentation, tests, user research notes, source code, configuration settings and files, and materials developed throughout this call order will be the property of the U.S. Government and in the public domain. One week prior to task order conclusion, all deliverables, products, will be incorporated into the project repository. Exclusion of project artifacts may be allowed in coordination with the OFA Product Owner and COR. Provide any other reasonable assistance to the Government to deploy the latest version application.

During the transition to the Government or a new contractor, the Contractor shall perform all necessary transition activities. Expected transition activities may include, but not be limited to:

- Continuation of full services to OFA and other customers
 - Participation in meetings with the Government or a new contractor to effect a smooth transition and provide detailed information on the operation of all deliverables, at COR and the OFA Product Lead's discretion.
 - Training of new personnel, either Government or a new contractor, during transition period
- Appropriate close-out of any outstanding technical and related performance elements for this task

Should the contractor be terminated prior to the end of the period of performance, the contractor shall transfer all project materials to the COR and the OFA Product Owner within two weeks of the COR and the OFA Product Owner's request.

2.0 List of Security Deliverables

Deliverable Name	Deliverable Title/Description	Due Date
Roster	Roster of all employees	Within 3 days of the effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)	Assist in the completion of a PTA/PIA form	Within 30 days after the contract award

Training Records	Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Rules of Behavior	Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident Response Report	Incident Report (as incidents or breaches occur)	As soon as possible and without reasonable delay and no later than 1 hour of discovery
Incident Response Plan	Incident and Breach Response Plan	Upon request from government
Personnel Security Responsibilities (onboarding)	List of Personnel with defined roles and responsibilities	Within 3 days that is before an employee begins working on this contract.
Personnel Security Responsibilities (off-boarding)	Off-boarding documentation, equipment and badge when leaving contract	Within 3 days after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract
Background Investigation Documentation	Onboarding documentation when beginning the contract	Prior to performing any work on behalf of HHS/ACF
Certification of Sanitization of Government and Government Activity-Related Files, Information, and Devices	Form or deliverables required by ACF.	At contract expiration
Contract Initiation and Expiration	If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan	At contract expiration
Security Assessment and Authorization (SA&A)	SA&A Package <ul style="list-style-type: none"> • SSP • SAR • POA&M • Authorization Letter • CP and CPT Report 	Due date to be determined and approved by ACF OCIO based on planned deployment and ATO schedule

	<ul style="list-style-type: none"> • E-Auth (if applicable) • PTA/PIA (if applicable) • Interconnection/Data Use Agreements (if applicable) • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other ACF-specific documents 	
Reporting and Continuous Monitoring	Revised security documentation/Agreements	As required by ACF OCIO
Security Alerts, Advisories, and Directives	List of personnel with designated roles and responsibilities	As required by ACF OCIO
Incident Reporting	<ul style="list-style-type: none"> • Incident Reports (as needed) • Incident Response Plan 	<p>Incident Response plan provided in accordance with ATO schedule and yearly thereafter (Prior to production deployment or go live date)</p> <p>Incident Reports provided quarterly and upon request</p>
Other IT Procurements (Non-Commercial and Open Source Computer Software Procurements)	<ul style="list-style-type: none"> • Computer Software, including the source code 	Prior to performing any work on behalf of HHS

3.0 Contract Provisions & Clauses

All provisions and clauses included and accepted as part of the vendor's GSA Schedule Contract flowdown to this RFQ.

Contractor Team Arrangement (CTA)

Contractor Team Arrangements (CTAs) are permitted. Note - FAR 9.6, Contractor Team Arrangements, does not apply to GSA Schedules teaming. Under GSA Schedules, Teaming allows contractors to use their individual GSA Schedules to develop a solution for the government.

{{If the vendor intends to team, a CTA is required by the closing date and time of the RFQ. However, a fully executed CTA will be formalized at time of award. CTAs shall utilize and submit this [Appendix 6](#) - ID231XXXXXX - Contract Team Agreement when a CTA is applicable.}}

CTAs will not be evaluated, but will be reviewed to:

- Gain an understanding of how the arrangement will work
- Identify any areas of responsibility that may require clarification
- Identify deficiencies in the CTA in order to understand the probability of successful performance
- Verify proposed prices/rates against MAS contract awarded prices/rates.

Contract Provisions

52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

<https://www.acquisition.gov/browsefar>

(End of provision)

GSAR 552.217-71 - Notice Regarding Option(s) (Nov 1992)

The General Services Administration (GSA) has included an option to [Insert “purchase additional quantities of supplies or services” or “extend the term of this contract” or “purchase additional quantities of supplies or services and to extend the term of this contract”] in order to demonstrate the value it places on quality performance by providing a mechanism for continuing a contractual relationship with a successful Offeror that performs at a level which meets or exceeds GSA’s quality performance

expectations as communicated to the Contractor, in writing, by the Contracting Officer or designated representative. When deciding whether to exercise the option, the Contracting Officer will consider the quality of the Contractor's past performance under this contract in accordance with 48CFR517.207.

(End of provision)

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)

52.204-26 Covered Telecommunications Equipment or Services-Representation (Dec 2019)

Contract Clauses

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/these address(es): (<https://www.acquisition.gov/browsefar>)

(End of clause)

FAR 52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation (Jan 2017)

FAR 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

FAR 52.212-4 Contract Terms and Conditions-Commercial Items (Oct 2018)

FAR 52.227-17 Rights in Data -- Special Works (DEC 2007)

GSAR 552.212-4 - Contract Terms and Conditions—Commercial Items (Feb 2018)(DEVIATION FAR 52.212-4)

GSAR 552.232-39 Unenforceability of Unauthorized Obligations. (FAR Deviation Feb 2018)

GSAR 552.238-82, Special Ordering Procedures for the Acquisition of Order-Level Materials

GSAR 552.204-70 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.

(a) Definitions. As used in this clause “covered telecommunications equipment or services”, “Critical technology”, and “substantial or essential component” have the meanings provided in FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing-

- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
- (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Representation. [Contractor to complete and submit to the Contracting Officer] The Offeror or Contractor represents that it [] will or [] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract, order, or other contractual instrument resulting from this contract. This representation shall be provided as part of the proposal and resubmitted on an annual basis from the date of award.

(d) Disclosures. If the Offeror or Contractor has responded affirmatively to the representation in paragraph (c) of this clause, the Offeror or Contractor shall provide the following additional information to the Contracting Officer--

- (1) All covered telecommunications equipment and services offered or provided (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);
- (2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision; 10

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of clause)

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

As prescribed in [4.2105\(b\)](#), insert the following clause:

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

(a) *Definitions.* As used in this clause—

“Covered foreign country” means The People’s Republic of China.

“Covered telecommunications equipment or services” means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

“Critical technology” means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

“Substantial or essential component” means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered

telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation [4.2104](#).

(c) *Exceptions*. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or

services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.217-8 - Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 calendar days before the contract expires.

(End of clause)

FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000)

- (a) The Government may extend the term of this contract by written notice to the Contractor within 5 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

(End of clause)