


SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NUMBER		PAGE OF 1 208	
2. CONTRACT NO.		3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER		5. SOLICITATION NUMBER 75P00124R00051		6. SOLICITATION ISSUE DATE 07/26/2024
7. FOR SOLICITATION INFORMATION CALL: 		a. NAME JACOB MATTHEWS			b. TELEPHONE NUMBER (No collect calls) 3852857382		8. OFFER DUE DATE/LOCAL TIME 08/15/2024 1200 ET
9. ISSUED BY OS/ASA/OAMS Office of Acquisition Management Services 5600 Fishers Lane 15E 10D Rockville MD 20857				CODE OAMS	10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input checked="" type="checkbox"/> SET ASIDE: 100.00 % FOR: <input checked="" type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB) <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB) <input type="checkbox"/> 8(A) NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 541214 SIZE STANDARD: \$39		
11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING 14. METHOD OF SOLICITATION <input type="checkbox"/> REQUEST FOR QUOTE (RFQ) <input type="checkbox"/> INVITATION FOR BID (IFB) <input checked="" type="checkbox"/> REQUEST FOR PROPOSAL (RFP)	
15. DELIVER TO CODE				16. ADMINISTERED BY See Schedule		CODE OAMS	
17a. CONTRACTOR/ OFFEROR CODE		FACILITY CODE		18a. PAYMENT WILL BE MADE BY CODE			
TELEPHONE NO. <input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER				18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	ADMINISTERED BY: OS/ASA/OAMS Office of Acquisition Management Services 5600 Fishers Lane 15E 10D Rockville MD 20857 USA (Use Reverse and/or Attach Additional Sheets as Necessary)						
25. ACCOUNTING AND APPROPRIATION DATA						26. TOTAL AWARD AMOUNT (For Government Use Only)	
27a. SOLICITATION INCORPORATES BY REFERENCE (FEDERAL ACQUISITION REGULATION) FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA						<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.	
27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA						<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.	
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.					29. AWARD OF CONTRACT: REFERENCE OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:		
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)			
30b. NAME AND TITLE OF SIGNER (Type or print)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (Type or print) ANNE M. MINEWEASER		31c. DATE SIGNED	

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
<input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL				
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY (<i>Print</i>)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		42b. RECEIVED AT (<i>Location</i>)	
		42c. DATE REC'D (YY/MM/DD)	42d. TOTAL CONTAINERS

B.1 BRIEF DESCRIPTION OF SERVICES

Requesting contractor support to provide operations and maintenance of an existing IT data and payroll and personnel processing functions including but not limited to IT pay generation, disbursement, and officer personnel system.

B.2 TYPE OF CONTRACT

The anticipated contract type is a Firm-Fixed Price

B.3 SEVERABLE SERVICES

The services acquired under this anticipated contract are severable services. Funds are only available for use for the contract line item (CLIN) to which they are obligated. Unused funds from one CLIN may not rollover for use in other periods.

B.5 CONSIDERATION AND PAYMENT

In consideration of satisfactory performance of the work as described throughout this contract, the Contractor shall be paid a fixed price for each CLIN (if exercised). If the options are exercised, funding will be obligated by modification to the contract. The base period and option periods are priced as follows:

Base Period - Period of Performance (PoP) Base Option CLIN 1001- November 1, 2024 to December 31, 2024 , Base CLINs 1002/1004: January 1, 2025 to July 1, 2025, Base CLINs 1003/1005: July 2, 2025 to December 31, 2025			
Base Period, CLIN 1	Description	Period of Performance	Fixed Price
Base Option CLIN 1001	Transition-In Services	2 Months	
Base CLIN 1002	Active Duty Personnel and Payroll	6 Months	
Base CLIN 1003	Active Duty Personnel and Payroll	6 Months	
Base CLIN 1004	Payroll/Personnel Policy Mandated Enhancements	6 Months	
Base CLIN 1005	Payroll/Personnel Policy Mandated Enhancements	6 Months	
Base Option CLIN 1006	Transition-Out Services	2 Months	
Base Option CLIN 1007	Ready Reserve Personnel and Payroll	6 Months	
Base Option CLIN 1008	Ready Reserve Personnel and Payroll	6 Months	

Option Period 1 - Period of Performance (PoP) January 1, 2026 – December 31, 2026			
Option Period 1	Description	Period of Performance	Fixed Price
Option Period 1, CLIN 2001	Transition-In Services	2 Months	
Option Period 1, CLIN 2002	Active Duty Personnel and Payroll	12 months	
Option Period 1, CLIN 2003	Payroll/Personnel Policy Mandated Enhancements	12 months	

Option Period 1, CLIN 2004	Transition-Out Services	2 months	
Option Period 1, CLIN 2005	Ready Reserve Personnel and Payroll	12 months	

Option Period 2 - Period of Performance (PoP) January 1, 2027 – December 31, 2027			
Option Period 2	Description	Period of Performance	Fixed Price
Option Period 2, CLIN 3001	Transition-In Services	2 Months	
Option Period 2, CLIN 3002	Active Duty Personnel and Payroll	12 months	
Option Period 2, CLIN 3003	Payroll/Personnel Policy Mandated Enhancements	12 months	
Option Period 2, CLIN 3004	Transition-Out Services	2 months	
Option Period 2, CLIN 3005	Ready Reserve Personnel and Payroll	12 months	

Option Period 3 - Period of Performance (PoP) January 1, 2028 – December 31, 2028			
Option Period 3	Description	Period of Performance	Fixed Price
Option Period 3, CLIN 4001	Transition-In Services	2 Months	
Option Period 3, CLIN 4002	Active Duty Personnel and Payroll	12 months	
Option Period 3, CLIN 4003	Payroll/Personnel Policy Mandated Enhancements	12 months	
Option Period 3, CLIN 4004	Transition-Out Services	2 months	
Option Period 3, CLIN 4005	Ready Reserve Personnel and Payroll	12 months	

Option Period 4 - Period of Performance (PoP) January 1, 2029 – October 31, 2029			
Option Period 4	Description	Period of Performance	Fixed Price
Option Period 4, CLIN 4001	Transition-In Services	2 Months	
Option Period 4, CLIN 4002	Active Duty Personnel and Payroll	10 months	
Option Period 4, CLIN 4003	Payroll/Personnel Policy Mandated Enhancements	10 months	
Option Period 4, CLIN 4004	Transition-Out Services	2 months	
Option Period 4, CLIN 4005	Ready Reserve Personnel and Payroll	10 months	

Contract Period	Fixed Price
Base Period Total	
Option Period 1 Total	
Option Period 2 Total	
Option Period 3 Total	
Option Period 4 Total	
TOTAL Potential Value Inclusive of all CLINS	

Payment shall be made upon the delivery and acceptance of the services required in accordance with the following payment schedules:

***Contractors to propose the Base payment schedules. Additional payment schedules may be proposed prior to exercise of any option or optional CLINS.

SECTION C - Description/Specifications/Statement of Work

C.1 PERFORMANCE WORK STATEMENT

Integrated Personnel and Payroll (IPP) Services for Officers of the Commissioned Corps (CC) of the U.S. Public Health Service (USPHS)

1 OVERVIEW

The United States Public Health Service is seeking vendor proposals to provide operations and maintenance of an existing IT data and payroll and personnel processing functions including but not limited to IT pay generation, disbursement, and officer personnel system. The current system interfaces with other HR systems and the US government Treasury department. The primary objective is to transition to a new service provider who will maintain the current IT technical services and to include the professional services for operations and maintenance of an existing payroll and personnel system data, output, and processing functions. This Performance Work Statement (PWS) outlines the requirements for transitioning to a new service provider while maintaining the existing IT data and payroll and personnel processing functions. The selected vendor must demonstrate expertise in system administration, project management, on-going IT support services, personnel and payroll processes and policies, cloud migration strategy and adherence to government regulations and standards. Compliance with the terms of service, SLAs, and performance metrics outlined within this PWS are essential for the successful execution of this contract.

2 TRANSITION AND OPERATIONS AND MAINTENANCE (O&M) SUPPORT

2.1 TRANSITION-IN PERIOD - There shall be a 60-day transition-in period initiated at the time of contract award. During this transition period, the contractor shall work with the Government and the outgoing contractor to minimize disruption of services and successful transference of personnel and payroll processing services.

2.1.1 During the Transition-In Period, the Government will require the Contractor to provide transition services beginning on an agreed upon date between the Government and the new contractor. During this period, staff from the incumbent supplier¹ and/or contractor shall be available to familiarize and train the new supplier staff to assume daily operations and maintenance by January 1, 2025. The new supplier's transition plan shall outline the supplier's methods and means to provide adequate coverage to ensure uninterrupted service, their process to manage the transition effectively and efficiently administratively for completion within 60 days post contract award.

2.2 COLLABORATION WITH OUTGOING CONTRACTOR

2.2.1 The new contractor shall work collaboratively with the outgoing-incumbent contractor service provider to ensure a seamless transition of the transitioned activities, including participation in transition meetings, coordination of the transfer of activities, and identification and accounting for other tasks required for a successful transition.

¹ Supplier and Contractor are used interchangeably throughout this Performance Work Statement.

- 2.2.2** Once the incoming contractor is fully operational, all outstanding/ accepted assessments by the Government will be transferred for completion by the incoming contractor.
- 2.2.3** The contractor shall be prepared to accept reviews at the conclusion of the Transition-In period.

2.3 CONDITIONS FOR TRANSITION COMPLETION

- 2.3.1** The contractor must successfully complete Government assessments and meet the following conditions, no later than 60 days post contract award (i.e., end of the Transition-In period), before the contractor is able to begin accepting and completing personnel and payroll processing tasks and operations.
- 2.3.2** All key positions, including but not limited to Project Manager, Software Developers/Programmers Software Architect, UI/UX Software Designer, Quality Assurance Specialist, SCRUM Master, Business Analyst, IT Security Specialist, Database Administrator/Programmer, and help desk support, for all labor categories have been fulfilled and/or security vetting and badging completed.
- 2.3.3** Obtain and maintain the Authority to Operate (ATO) for a Secure File Transfer Protocol (SFTP) data server and/or other methods approved by OASH IT Services to receive payroll and personnel data.
- 2.3.4** Obtained the required connectivity to the various systems i.e., Treasury Department, refer to SLA attachment included for detailed connections required.

2.4 O & M SUPPORT

This section is dedicated to outlining the required ongoing operations and maintenance (O&M) support services to be provided by the new contractor after the successful transition period. The contractor is expected to ensure the continued functionality, security, and reliability of the personnel and payroll processing, IT and Administrative functions including but not limited to:

- Regular system maintenance and updates
- Helpdesk support for users
- On-going operations
- Incident management and resolution
- Security monitoring and compliance
- Performance optimization
- Disaster recovery planning and execution
- Documentation maintenance and updates
- Collaboration with government stakeholders for system enhancements and improvements
- Adherence to service level agreements (SLAs) and performance metrics outlined in the contract.
- The contractor should provide detailed plans, procedures, and resources for executing these O&M support services effectively and efficiently, ensuring the uninterrupted operation of the IT systems and compliance with all relevant regulations and standards.

3 KEY TECHNICAL TRANSITION REQUIREMENTS AND PROPOSAL ELEMENTS

- 3.1** Transition Process and Schedule: Detailed schedule for transition of IPP processing and associated functions including major/minor milestones ensuring completion within no less than 60 days.
- 3.2** During the Transition-In period, the Contactor will define the roles and responsibilities of the new contractor, existing vendor, and government agency including communication channels, tools, and escalation methods.
- 3.3** System Administration and Project Management Support: Program Management Plan (PMP) defining organizational resources, processes, and procedures associated with program management and execution.
- 3.4** Establishment of reporting forums aligned with processes to report on task status and ensure full disclosure of execution progress.
- 3.5** Quality Management: Perform quality assurance as a process, monitoring the overall plan, procedures, and controls to maintain a satisfactory quality system.
- 3.6** On-going Support Services: Program Roadmap/Schedule in accordance with the PMP, including key decisions, software life cycle activities, test activities, integration activities, training activities, task dependencies, and risk reduction/mitigation activities.
- 3.7** Risk Management: Establish, document, and conduct a risk management process in compliance with HHS standards that mitigates program risks during transition, assumption of IPP processing and associated functions and provides metrics to monitor risk status.
- 3.8** Conditions for Successful System Handover: Uninterrupted payroll and personnel services and/or processes ensuring continuity of operations.
 - 3.8.1** Success Factors:
 - 3.8.1.1** All critical functions to process personnel and payroll are operational.
 - 3.8.1.2** Data integrity is maintained throughout the migration process.
 - 3.8.1.3** Users can access and utilize the personnel and payroll system without system disruption.
 - 3.8.1.4** Adequate training is conducted for relevant stakeholders to ensure operational proficiency with the payroll and personnel system.
 - 3.8.1.5** Success completion of payroll and personal solution test by December 16, 2024
 - 3.8.1.6** Complete security testing and assessment against threats and vulnerabilities.
- 3.9** Compliance with government financial stewardship regulations.
- 3.10** Compatibility with existing infrastructure and data maintenance.
- 3.11** Potential Teaming or Subcontracting Arrangements supporting, 4–8-week transition window, base year and up to 4 option year periods.
- 3.12** Training and Knowledge Transfer: Identification of training needs for the new vendor's staff, incumbent vendor, and government personnel involved in the transition, including the transfer of knowledge and associated documentation (user manuals, how to guides etc.).
- 3.13** User Manuals and How-To Guides. The contractor shall create user manuals and/or How-To guides to document the processes and/or functions for the new provider's personnel and payroll solution.
- 3.14** Procedures for Quality Assurance, Testing, and Validation: Testing and validation procedures ensuring accuracy of data, security, and system reliability upon completion of the transition.

- 3.15** Identification of Potential Risks and Mitigation Strategies: Identification of potential risks and challenges with the transition process, with outlined mitigation strategies to minimize disruption and ensure continuity of services.
- 3.16** Terms of Service, Service Level Agreements, and Performance Metrics: Service Level Agreements (SLAs), performance metrics, and dispute resolution mechanisms.
- 3.17** Government Requirements (GFI/GFE): The contractor will utilize hardware, software, and IT services provided and/or approved by the Government to support the services required in this PWS. The contractor will be restricted to the use of Government-provided software applications and tools, with justification and Government approval for additional and/or external applications and tools.
- 3.18** Program Management activities will span all contract tasks, including establishment and implementation of a Program Management Plan (PMP), Contractor Quality Control Plan (QCP), and risk management processes.
- 3.19** Cloud Migration Strategy: Describe the strategy for migrating the existing system to the cloud, including ATO certification costs and successful industry approaches to transition support and services.
- 3.20** Additional Information Required for Cost Proposal: Identify any additional information required by the offeror to propose estimated costs for transition and O&M.

4 INTRODUCTION

The U.S. Public Health Service Commissioned Corps (USPHS) is an elite team of more than 6,000 full-time and reservist of well- trained, highly qualified public health professionals dedicated to delivering the Nation's public health promotion and disease prevention programs and advancing public health science. Corps officers serve in a variety of positions throughout the U.S. Department of Health and Human Services (HHS) and certain non-HHS Federal agencies and programs that focus on key areas of disease control and prevention; biomedical research; regulation of food, drugs, and medical devices; mental health and drug abuse; health care delivery; and international health.

As one of America's eight uniformed services, the Commissioned Corps fills essential public health leadership and service roles within the Nation's Federal Government agencies and programs. The Corps has officers in many professions, including:

- Physician
- Nurse
- Dietitian
- Health Services Officer
- Scientist/Researcher
- Veterinarian
- Dentist
- Pharmacist
- Engineer
- Environmental Health Officer
- Therapist

5 SCOPE OF WORK

The Department of Health and Human Services (DHHS) is seeking a vendor to provide operations and maintenance of existing IT data and payroll and personnel processing functions including but

not limited to IT pay generation, disbursement, and officer personnel system. The vendor's proposed solution system must be able to handle the collection of source documents, determination of all pay categories, gross-to-net calculations, and interface with all the various internal and external systems required to ensure the accurate disbursement of personnel resources, funds, and administration & maintenance of all related IT systems. Once successfully implemented, the system needs to be kept current: both for policy mandate updates, routine pay table adjustments and for changes to pay calculations as mandated by the Secretary of DHHS or Congress.

The scope of work includes validating the requirements with each Branch, the development of user stories, operations/process support, timeline management and workflow changes necessary to complete deliverables.

The Contractor is expected to draw on established methods, best business management solutions, practices, and Government/industry experience in applying application.

The system must provide functionality to meet the following current capabilities:

- Capability Goal 1: Scalable Platform with Business Intelligence
- Capability Goal 2: Accelerate Technology Modernization and Innovation
- Capability Goal 3: Enhance Data Integration and Networking
- Capability Goal 4: Data Management and Interoperability
- Capability Goal 5: Improve IT Management, System Standardization & Governance

The following are required functions that are performed for the Active duty, Ready Reserve and Retiree on the payroll and personnel system:

- Active-duty payroll
- Adverse Actions
- Assignments
- Awards
- Credentialing
- Electronic Official Personnel Folder (eOPF) DD214/215 Management
- Immunizations Tracking
- Leave & Absence Tracking
- Licensure tracking
- Medical Readiness
- New Hire/Call to Duty
- Officer Payroll Processing
- Officer profiles
- Officer self-service
- Agency Position Management
- Officer Promotions
- Readiness and Deployment compliance
- Retirements & Separations
- Security Clearance Tracking

6 BACKGROUND

Payroll services are currently provided in-house human resources (HR) personnel of U.S. Public

Health Service (USPHS) Commissioned Corps Headquarters (CCHQ) using a cloud-based software system, that collects data from source documents through user-accessible transactions, calculates gross compensation as well as gross-to-net disbursements. Personnel orders are processed by the HR staff who collect records, maintain files, and perform personnel related transactions using the integrated personnel order and payroll system.

HR personnel are responsible for overseeing payroll operations and transaction. The Office of Assistant Secretary of Health (OASH) IT Services is responsible for overseeing development, integration, modification, or operations and maintenance of OASH's information ecosystem. CCHQ is responsible for the overall procurement, administration, management and/or operations and maintenance of the integrated personnel order and payroll system by overseeing the production of the USPHS Commissioned Corps officer's payroll using the existing cloud-based software system. After each monthly payroll is computed, validated, and certified, Financial Services Branch (FSB) within CCQH transmits all payroll to the Department of Treasury for disbursement as part of post payroll transactions and tasks.

Commissioned Corps Personnel and Payroll System (CCP). CCP is the web-based, real-time, workflow enabled, personnel and payroll management system providing electronic initiation and processing of military personnel actions, computing compensation, and maintaining personnel and payroll records for Active duty, Ready Reserve, and retired Officers of the USPHS Commissioned Corps. The CCP system provides a full range of services from call to duty through Retirement/resignation.

OASH IT Services is responsible for maintaining all Corps-specific information technology systems including COPS10GDB and subsystems e.g. CCMIS, Payroll, Readiness (COER), AES/ATS, and HR Applications, that support officer recruiting, call to duty, separations, retirements, promotions, assignments, readiness, deployment, including the public-facing USPHS website (www.usphs.gov), and the business operations site (dcp.psc.gov) through which officer records and leave management systems are accessible. Dashboard for Leave Management and tracking per unit or region. Leave management is currently also accessible directly via phsleave.lyceum.com. Regarding payroll, the OCIO collects records, maintains files, audits individual payees, performs payroll transactions using CCP and administers a system of basic pay, allowances, and special or incentive pay for active duty USPHS officers. The Financial Services Branch provides these services in coordination with the Departments of Defense (DoD), Department of Veterans Affairs (VA), Coast Guard, United States Department of the Treasury Personnel Support Center, and Social Security Administration. Commissioned Corps Headquarters (CCHQ) collects records, maintains files, and performs personnel related transactions using the existing solution.

7 CURRENT SYSTEM OVERVIEW

The current payroll and leave system are a web-based application running on servers housed in an off-site collocation facility. It provides for data input from personnel and payroll source documents. The transactions are edited at point of origin and then combined with any other input documents for that employee to determine all changes since the last instance. Pay determination is by exception only; the default is to receive the same pay as the previous (monthly) cycle. In addition to proactive changes, the system can detect changes due to longevity milestones. These longevity changes occur for both base pay and several types of specialty pay to which an officer may be entitled.

The system stores large tables provided by the Department of Defense (DoD) to determine the amount of housing allowance to which officers are entitled based on their grade, dependent status, and duty station zip code. Because officers can be called to duty, transferred, or separated at any point during the payroll cycle, the system must be able to determine prorated earnings for all categories of pay. As supporting documentation may arrive after the fact (e.g., change in marital status), the system shall be able to perform retroactive adjustments for, at a minimum, all pay cycles in the current tax year. The replacement system should be web-based using modern tools according to accepted standards. It must allow for different levels of administrative and user roles and responsibilities. Certain transactions that do not affect an officer's gross pay (e.g., tax withholding, payroll address, savings allotment) should be available via Self-Service.

Transactions that require review and approval (e.g., dependent certification) should be initiated by the officer and forwarded to a payroll technician before being finalized. Other transactions (e.g., bonus pays) are initiated and/or approved by members of the officer's organization prior to being forwarded to the payroll technician. The system should display an earnings statement on the web that shows each element of pay, both current and year-to-date, indicate whether the element is taxable or non-taxable, and each deduction and allotment to gross pay. Before the end of January each year, the system should display the officer's W-2 statement. Both the earnings statement and W-2 should be available for printing. The database engine should be accessible for standard and ad-hoc reports using commercially available packages.

The current system stores all the data necessary to perform gross-to-net calculations and maintain both taxable and non-taxable earnings. It performs federal, state, and local tax calculations using tables provided by a third-party vendor. It creates output files for Electronic Funds Transfer (EFT) transactions to banks, insurance companies, Thrift Savings Plan, charities, U.S. Savings Bonds, tax entities, etc. It provides output data in a format suitable for auditors and historical review. It does not disburse funds but rather provides data to the U.S. Treasury in predefined formats. The existing system has interfaces to numerous internal and external data systems from varying technology platforms and solutions.

8 CONSOLIDATED SYSTEM OVERVIEW REQUIREMENTS

The Offeror shall continue to provide a consolidated solution for the USPHS Commissioned Corps Personnel, Readiness, Deployment and Payroll system to comply with the personnel and payroll processing requirements of the United States Public Health Service, also known as the Commissioned Corps. This consolidation places USPHS Commissioned Corps personnel processing, Active-Duty payroll, Ready Reserve payroll under one system. A single, standardized system that consolidates USPHS Commissioned Corps personnel and readiness processing, active-duty payroll, and ready reserve payroll reduces security risks and cost. The Contractor shall provide the necessary skilled staff to perform the following services:

8.1 PERSONNEL PROCESSING

The U.S. Public Health Service Commissioned Corps Headquarters (CCHQ) has consolidation and migrated payroll and certain essential personnel functions to one system. The following personnel processing functions have been migrated and currently operates in a cloud-based environment.

- Active-duty payroll

- Adverse Actions
- Assignments
- Awards
- Credentialing
- Electronic Official Personnel Folder (eOPF) DD214/215 Management
- Immunizations Tracking
- Leave & Absence Tracking
- Licensure Tracking
- New Hire/Call to Duty
- Officer Payroll Processing
- Officer Profiles
- Officer Self-service
- Position Management
- Promotions and Evaluations
- Readiness Compliance
- Retirements & Separations
- Security Clearance Tracking

Upon receipt of source documents, personnel transactions are entered by the Human Resource Specialists (HR Specialist – Military) in the Assignments Team of the Commissioned Corps Headquarters (CCHQ) into the same software system that is fully integrated with the payroll system. The data from the software system will be system-agnostic. Because many personnel transactions immediately affect pay, vendors shall describe how the offered solution will continue to shall integrate personnel transactions with pay rules. Within a given month, no less than 1500 personnel transactions processed. Vendor shall meet with Financial Services and other operational Branches to identify capabilities and develop solutions for continuous self-service personnel and payroll functionality.

9 MANDATORY FUNCTIONALITY REQUIREMENTS

The following are mandatory continued functionality and continuity of service requirements for the new provider solution at time of Transition and/or Go-live:

9.1 ASSIGNMENTS

The assignments include transactions run as a result of: Transfers (Permanent Change of Station), Position Updates, Temporary Duty assignments, Amendments to personnel orders, Cancellation of personnel orders, Prior Service Data Management (both Active Duty and Civil Service), Duty Station Address Changes, ADMIN Code Changes, Board Certified Pay, Name Changes, Extension/Removal of Limited Tours, Retirements, Separations/Terminations, Promotions, Miscellaneous Orders, Active Duty Deaths, Close Out Personnel Orders, Electronic Official Personnel Folder (eOPF) DD214/215 Management, Board Member Appointments & Extensions, AWOLs, Non-Duty with Pay, Blanket/Individual Details, Long & Short Term Training, PIR Correction and maintenance, Licensure Database, Lump Sum Leave calculations and Statement of Services (following Active Duty, Ready Reserve, Retirement or Separation).

9.2 SYSTEM GENERATED SIGNATURE

The solution shall provide the functionality for a system generated signature for the CCHQ Director in the issuance of Personnel Orders. The contractor shall provide and execute the functions needed to add additional system generated signature fields as needed.

9.3 LEAVE & ABSENCE TRACKING

Leave and absence tracking shall be fully integrated in the offered system as per the policies and procedures related to annual leave for officers in the Commissioned Corps of the U.S. Public Health Service dcp.psc.gov/ccmis/ccis/documents/CC362.01.pdf. Additionally, an on-line leave and earnings statement will be available for viewing and printing by the active-duty and ready reserve officers through their self-service accounts. The consolidated administrative system should allow HR Specialists to enter and manage, store the necessary documentation for, and produce reports on, current Leave and Absence for each active-duty and ready reserve officer. The consolidated administrative system should include a form 1373 automation feature for terminal leave processing by the

Personnel Career Management and Separations and Assignment Branches. The design should include the development of users stories, timeline management and workflow changes. The consolidated administrative system should provide for an extension of the Terminal Leave function. This enhancement should include the automation of the functions used in the Separation Process in accordance with Policy (CCI 387.01 – Separation of Commissioned officer).

The offered solution shall provide an application whereby Active Duty and Reserve Corps officers who are considering separation, can request a current report, showing their unique data. This application must individually determine a retiring officer's pay rate is through a Retirement Calculator function.

These functions automate the manual processing currently performed by staff in the Medical Affairs, Personnel Career Management, Financial Services and the Separations and Assignment Branches. The scope of work includes the development of user's stories, operations/process support, timeline management and workflow changes necessary. The scope of work should include the development of user stories that eliminate errors and prepare all documents; timeline management and workflow changes necessary to complete deliverables in addition to a testing environment for stakeholders. In addition, the system shall provide the leave approver/designee with a collective leave calendar of all leave for all officers assigned to the approver.

9.4 DIVESTMENT ANALYSIS

The consolidated administrative system should provide for an extension of the Terminal Leave function. This functionality should include the automation of the functions used in the Separation Process in accordance with Policy (CCI 387.01 – Separation of Commissioned officer).

The offered system shall provide an application whereby Active Duty, Ready Reserve officers, who are considering separation, liaisons, and CCHQ Separation Specialist will be provide a report containing the unique data of the Separating officer. This application must individually determine the separating officer's pay rate is through a Retirement Calculator function. When encountering a resignation, the application will utilize source data and Commissioned Corps business rules to compute the creditable service time, any Officer indebtedness based on service or financial obligation contracts (long-term training, special pays, etc.). Upon completion, the offered system must produce a report indicating what will occur upon resignation, retirement or termination as well as provide data metrics reporting that is editable and exportable. The scope of work should include the development of user stories that eliminate errors and prepare all documents, timelines management and workflow changes necessary to complete deliverables and provide a sandbox and test platform for users to interface before going live to production.

9.4.1 DD-214 INTEGRATION

The consolidated administrative system should include an electronic integration whereby officer's work history and other data are electronically

and securely transferred to downstream applications, including the DD214. The DD-214 integration should include access on the self-service portal for retired/separated officers. The offered solution will continue to include a curated set of data analytics formatted for easy ingestion to 1) measure progress towards Force Distribution and 2) facilitate resultant actions to drive alignment with Force Management policy mandates.

9.5 OFFICER SELF-SERVICE

The consolidated administrative system will include a self-service module that will allow Officers secure access to manage a wide range of activities including adding and updating contact information, view payroll data and forms (e.g., monthly payroll information and transactions, federal and state forms). The designed system will include a dashboard for Helpdesk Self and Financial Services Branch to manage incoming officer requests. The self-service will allow officers access to view their payroll data (W4, state tax, allotments, net check to bank, etc.), and online access to view, print and manage personal information at any time and from mobile devices. Additionally, the self-serve system should include functionality for End of Year (EOY) Social Security Adjustments which will include functionality for moving OASDI to Indebtedness Loan.

THE RANGE OF SELF-SERVICE FUNCTIONS MUST INCLUDE:

- Absence/Leave Requests
- Benefits
- Contact Information
- Demographic Data
- Education
- Emergency Contacts
- Active Duty Pay
- Retirement Information
- Tax Set-Up Information
- Thrift Savings Plan (TSP) Change Function
- Peer Review of Results
- IRS and SSA Reporting
- Employment Verification Letter
- Cost Estimation Letter
- DD214 for retirees/separated officers

9.6 OTHER SELF-SERVICE

The consolidated payroll and personnel administrative system will include Other Self-Service module that will allow Officers secure access to manage a wide range of activities. The range of functions must include:

- Personal awards
- Award Eligibility
- Position history
- Readiness compliance

- Officer Mobilization and Deployment Tracking
- Deployment Orders Dashboard
- Security clearance
- Skills and training
- Immunizations
- License & certifications
- Medical examinations
- Upload of Transcripts for degrees acquired after the Call to Duty

9.7 POSITION MANAGEMENT

The consolidated payroll and personnel administrative system will include a position management function that separates the concept of a position from that of a job and a person in a role. The position management function must provide to the HR Specialist of CCHQ the ability to add, modify, store and report on the organization structure, jobs, and unique attributes and associated number of a position. The system must have an efficient process to create and maintain positions, as well as display all officers in a position across our entire organization.

9.7.1 1662 AUTOMATION

The consolidated administrative system should automate the 1662 Personnel Action Form. The outcome is a digitized and streamlined process that modernizes user interactions with standard administrative tasks, such as CAD, Billet Change, Transfers, etc. This automation should remove much of the manual processing done by the Call to Active Duty and Recruitment, Personnel Career Management, Reserve Corps and Separations and Assignment Branches. The offered solution will continue to shall include data analytics enabling transparency, management oversight and visibility. The scope of work includes development of user stories that eliminate errors; preparation of all forms; integration with officer's electronic folders; timeline management and workflow changes necessary to complete deliverables

9.8 READINESS AND DEPLOYMENT COMPLIANCE

The consolidated administrative system will allow the Medical Affairs data entry team to update an officer's profile with new information on Medical Evaluation, Immunizations and Licensure and Certification.

Active-Duty and Ready Reserve officers must be given the opportunity to view their present and projected readiness status and maintain the information necessary to achieve a basic-level of readiness. These include Annual Physical Fitness Test, Basic Life Support, Deployment Role, Five-Year Medical Evaluation, Immunization, Licensure and Certification, and Waivers (medical and non-medical).

If an officer's current or projected readiness status is not compliant, the system must clearly show the officer the specific reason for non-compliance to facilitate correction. The HR Specialist of CCHQ must be allowed to view all readiness compliance information in accordance with USPHS standards.

9.9 ACTIVE DUTY AND READY RESERVE PAYROLL

The Commissioned Corps operate two payrolls on an exception-based nature, determining monthly pay for Active Duty and Ready Reserve Officers. The offeror's solution shall produce timely and accurate pay on a monthly basis for all 6,000+ Active Duty and Ready Reserve Officers. The descriptions below provide a conceptual overview of the key components of the desired payroll solution.

9.9.1 Payroll Calendars & Pay Statement

For active-duty officers, each pay period begins on the first day of each calendar month with officers being paid on a 30-day month. That is, payday for active-duty officers is typically the first day of the following month, or the previous workday, if the first day of the month is not a workday. In rare cases, Active-duty officers are paid twice in December on the first and last workday of the month. Pay statements will be mailed monthly to be received by officers no later than the first day of the following month.

9.9.2 Calculation Engine

9.9.2.1 Pay Rules

- The offeror's payroll engine shall support the Commissioned Corps pay rules including, its payee classes, wage tables, source to net calculations and post-tax computations. In accordance with Congressional mandates, rules may be added, removed, or amended to fit changing criteria within the Corps.
- Pay rules shall work in conjunction with the 300+ Nature of Actions (NOAs) – the payroll and personnel transactions – used by the Payroll Technicians and HR Specialists who process changes to selected Officer's pay daily.
- Pay rules shall support Special Pays as applied to the various categories of Officers, including Medical, Dental and Contract Special Pays.

9.9.2.2 Retroactive Processing

The offeror's solution must support retroactive processing such that transactions may be entered with effective dates prior to the current period, even prior periods in earlier tax years. In this event, the offeror's system shall calculate the adjustments to pay.

The collection of retroactive overpayments shall be negotiated with the Officer in accordance with Commissioned Corps policies and procedures, while the disbursement of retroactive underpayments shall be taxed in the current period, in accordance with IRS

regulations, specifically those documented in IRS Publication 15, Circular E: Employer's Tax Guide.

9.9.2.3 Future Dated Processing

The offered solution will continue to support transactions entered with effective dates in future pay periods, even in subsequent tax years. In this event, the offeror's system shall calculate the adjustments to pay when that future period becomes effective.

9.9.2.4 Annual Calculations

Once successfully implemented, the offered system must be kept current, both for routine pay table adjustments and for changes to pay calculations as mandated by the Secretary of DHHS or Congress. The offered solution will continue to support annual adjustments to the following tables which inspire calculations to all payees: Base Area Housing (BAH), Base Area Subsistence (BAS), Base Pay, Cost of living adjustment and the Veteran's Administration benefits. In addition, the solution shall support adjustments to standard amounts for FICA, Thrift Savings Plan, Taxes, etc.

9.9.3 Active-Duty Transaction Processing

The modification of pay is by exception only; the default is to receive the same pay as the previous (monthly) pay period. The likely cause of a pay change is modification to the Officer's data, caused by execution of a transaction – known as a Nature of Action, or NoA. Within a given month, the number of transactions processed range from a minimum of 2,500 to twice that amount, and possibly more. The offered system shall be structured to support this processing capacity.

Transactions are categorized by type and belong to four (4) functional areas: Compensation, Personnel, Retirement and System.

9.9.3.1 Active-Duty Compensation

Payroll services are currently managed by the Payroll Technicians within the CCHQ, FSB using a proprietary software system with a web-based graphical user interface. Vendors shall replace this system, which collects data from source documents summarizing

changes to pay. These transactions fall within the following categories:

- Administrative – One-time payment, Payroll Address Change, etc.
- Entitlements – Lump Sum Leave, Quarters Allowance, etc.
- Deductions – Bonds, Charity Allotment, Federal/State taxes, garnishments, etc.
- Benefits– Insurance Allotment, Life Insurance, Thrift Savings Plan, etc.
- Retirement – Retire an Active Duty Officer, Start/Stop retirement pay, Annuity setup, former spouse setup, etc.
- Special Pays – Accession Bonus, HPSP, Hazard Duty, Imminent Danger, etc.

9.9.3.2 Active-Duty and Ready Reserve Personnel

Upon receipt of source documents, personnel transactions are entered by the Human Resource Specialists (HR Specialist) of the CCHQ Assignments into the same proprietary, software system is fully integrated with the payroll system. As many personnel transactions immediately affect pay, vendors shall describe how the offered solution will continue to integrate personnel transactions with pay rules. Within a given month, the number of personnel transactions processed range from a minimum of 1,500 to twice that amount, and possibly more.

The number of personnel transactions fall within the following categories:

- CAD – Call to Active Duty, Assimilation into Regular Corps, etc.
- Transfer – from/to Billet, Program and/or Station, etc.
- Grade Change – Permanent or Temporary Promotion or Reversion
- Separation – Death, Termination, or Retirement
- Miscellaneous – Address Change, Permissive Order, etc.
- Other – Long-Term Training, Short-Term Training, Statement of Service.

9.10 Workflow Processing

9.10.1 Peer Review

Each transaction updates different data elements. The data elements modified in each transaction must be viewed and validated by at least 2 experienced personnel within CB or DCCA. Given the volume of data changes and transactions processed each month, the HR Specialists and Payroll Technicians have come to rely on an ordered peer review and supervisory approval (workflow) process. Within workflow, data changed in each transaction undergoes peer review, and possibly supervisory approval, before being permanently committed to the database.

9.10.2 Personnel Orders

For personnel transactions, the offered system shall produce an accompanying legal document

A Personnel Order (PO) document – typically fitting on a single sheet of paper, which shall be electronically stored on each officer's record within the system. The contents of the PO shall differ from transaction to transaction, reflecting the transaction type, data elements within the transaction and the individual data of that Officer. Each PO shall be finalized and stored only after the transaction has successfully been processed through the peer review and supervisory approval stages. Secure access to personnel orders by users with differing roles is mandatory requirement of the offered solution.

9.10.3 Personnel Order Close Process

For personnel transactions, the offered system shall produce an accompanying Personnel Order (PO) document – typically fitting on a single sheet of paper, which shall be electronically stored on each officer's record within the system. The contents of the PO shall differ from transaction to transaction, reflecting the transaction type, data elements within the transaction and the individual data of that Officer. Each PO shall be finalized and stored only after the transaction has successfully proceeded through the peer review and supervisory approval stages the PO CLOSE process.

For personal transactions, the offered system shall interconnect the CCP and eOPF systems such that personnel orders and supporting documents are processed and stored electronically, without manual intervention (printing, scanning, or filing). Specifically, the system must allow Reviewers of Nature Actions (NoA) to upload files (supporting documents) to the NoA such that the files will be stored along with Personnel Order (PO).

9.10.4 Personnel Order Amendment Process

From time-to-time new information is received regarding a CLOSED transaction, forcing that transaction to be significantly modified, invalidated, or run on a different effective date. The vendor shall describe how the offered solution will continue to support this requirement.

9.10.5 Personnel Data – ORACLE Interface

The data modified by transactions that are in CLOSED status are electronically transmitted to the Commissioned Corps Management Information System (CCMIS) application on a periodic basis. The offered system should support this real-time transfer of data using a secure interface, preferably the SOAP protocol.

9.10.6 Retirement from Active Duty

The Commissioned Corps operates two payrolls on an exception-based nature, determining monthly pay for Active Duty and Retired Officers. Each month approximately 10 to 45 officers retire from Active Duty and shall begin to receive pay in accordance with one of four retirement plans: Final Pay or High 36, Redux/CSB, Blended Retirement.

In addition, officers may retire on temporary or permanent disability. A retiring officer's pay rate is individually determined through a Retirement Calculator function that utilizes source data and Commissioned Corps business rules to compute the creditable service time. This calculator simultaneously functions as a base pay determination for officers newly on active duty, who have creditable service to begin receiving pay at the appropriate level. The offered solution will continue to support both active duty and retirement functions of the Retirement Calculator, its rules, processes, and reports.

The consolidated administrative system should provide for an automation of the Mandatory and Medical retirement as well as Involuntary Terminations. These functions should automate much of the manual processing done by the Medical Affairs, Personnel Career Management and Separations and Assignment Branches. The scope of work should include the development of user stories that eliminate errors and prepare all documents; timeline management and workflow changes necessary to complete deliverables.

9.10.7 Blended Retirement System

On January 1, 2018, the modernized retirement system for members of the uniformed services, commonly referred to as the Blended Retirement System (BRS) was instituted. BRS consists of four components that distinctively combine to deliver a new blended annuity package categorized by the following:

- Defined Retirement Pay Benefit
- Thrift Saving Plan (TSP) Automatic and Matching Contributions
- Continuation Pay
- Lump Sum Retired Pay Payment

9.10.8 Requirements Gathering

In the planning (or requirements gathering) phase, the Vendor is to obtain accurate descriptions of the Government's objectives and obtain an accurate understanding of the relevant technical details to successfully document the desired result(s). The Government will provide its objectives and requirements to the Vendor. Once received, the Vendor will prepare specifications and other documentation based on its understanding of the Government's requirements and deliverables. In this phase, the Vendor shall develop questions and create functional specifications for development.

Following the Government's approval of functional specifications, the Vendor will move to its next phase: Modification and Software Development.

9.10.9 Work Plan/Timeline

Work required to support the Blended Retirement system is included as part of the CCPayroll solution. BRS development work shall be subject to the standard terms of our Contract and may include a modification.

9.11 Retirement Tracking System

In the months preceding retirement, personnel within the CCHQ and OCIO begin to identify, gather, and store specific information regarding retirement candidates. The process of retirement within the offered system is known as the Retirement Tracking System (RTS). The RTS is an integral function of the pay and personnel system of the Commissioned Corps, and as such a mandatory requirement of the offered solution

9.12 Retired Pay Compensation Transactions

Pay for the 6,100+ retired officers, annuitants, and former spouses is also calculated on an exception only basis in accordance with the rules prescribed in Chapters 71 and 73, Title 10, United States Code. The default is to receive the same pay as the previous (monthly) pay period, however, modifications to pay tables, external compensation or tax tables are often changed. The offered solution will continue to support the computation of retired pay.

Retiree transactions are categorized by type and belong to seven (7) functional areas (see below): Annuitant, Death, Disability, Former Spouse, Other, Retired Officer and VA/Concurrent Receipt.

9.13 Monthly Payroll Processing

9.13.1 Payroll Calendar

Each pay period begins on the first day of each calendar month with officers being paid on a 30- day month. That is, payday for active-duty officers is typically the first day of the following month, or the previous workday, if the first day of the month is not a workday. In some years, Active-duty officers are paid twice in December on the first and last workday of the month.

9.13.2 Payroll Master Files

Upon completion of payroll, the offered system shall produce several master files containing pay, personnel, and benefit data. These master files are known as the XMaster, COMaster and D&L respectively. The offered system shall support the requirements of the Payments and Accounting Team, who are responsible for payroll reconciliation each month. A package of reports shall also be made available to the team.

9.13.3 Payroll Data Files

Officers may purchase Series I and Series EE Bonds in available denominations through payroll deduction. The offered system shall create a Bond Payment file that can be used to transmit payment information in accordance with the rules of the United States Treasury department.

9.13.4 Interface Files/Reporting

The existing systems have interfaces to numerous internal and external data systems, including DEERS, 3rd Party, TSP, VA, etc. In addition, data in the offered solution will continue to accept input from and export data to several existing Oracle applications supported by the CCSB staff. These include the database tables supporting the applicant system, the electronic call to active-duty system, the promotion system, the officer evaluation system, etc.

10 Data Structures: Initial Load & Updates Requirements

The database used within the offered system shall be structured to store a myriad of actionable information, including Admin Codes, Bank Routing Nos., Bonus Amounts, Common Accounting Numbers, GEO Codes, Special Pays, State Tax Amounts and the like. Several of these tables are updated monthly, including DEERs, etc. Other records are updated on an annual basis, including Base Pay tables, Base Area for Housing, BAS, Cost of Living Allowance, etc.

11 Audit Requirements

Given the magnitude of transactions processed by Payroll Technicians and HR Specialists, the offered solution will continue to support a system-based audit trail. In addition, the offeror shall provide technical expertise or facilitate technical resources to support the ongoing Government audit programs as prescribed by DHHS.

11.1 Audit Trail

Each data entry, action and event shall be time-stamped, providing a complete access to an historical audit trail, and enabling tracking of input errors.

11.2 C&A: Security Certification and Security Accreditation

As mandated by DHHS, OASH officials must undergo an annual Certification and Accreditation (C&A) program, in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. The information security program must include periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls. This testing should be performed with a frequency depending on risk, but no less than annually.

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, that determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision. The offeror shall support AOS in its performance of the Certification and Accreditation of the CCP system.

11.3 SSAE 16 Type II Examination replaces SAS 70

The Government Management Reform Act (GMRA) expanded the CFO Act of 1990 to require the issuance of audited financial statements by DHHS and other agencies.

Under the DHHS plan to implement GMRA, the OASH is required to complete an annual examination of the CCP system. The auditors have determined that independent examinations of internal controls shall be completed annually under the guidelines of the American Institute of Certified Public Accountants Statement of Auditing Standards (SAS) Number 70, Reports on the Processing of Transactions by Service Organizations. The annual examination is a “Type 2” report providing an opinion on the internal controls placed in operation and includes tests of operating effectiveness.

The SAS 70 examination shall result in the issuance of reports on controls placed in operation and tests of operating effectiveness in accordance with AU § 324.41 324.57. The period of examination is October 1st of the current year, through June 30th of the following year. The scope of the engagement shall cover all controls and processes required by FFMIA criteria and relevant governing agencies, such as Treasury or OMB, as applicable to SAS 70 testing procedures, up to and including:

- Elements of Internal Controls
- Systems Development Life Cycle (SDLC)
- General Computer Controls
- Additional General Controls
- Application Controls

11.4 Material Controls

SSAE 16 SOC 1 reports, which have effectively replaced SAS 70 reports as of June 15, 2011, will be prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. SOC 1 reports retain the original purpose of SAS 70 by providing a means of reporting on the system of internal control for purposes of complying with internal control over financial reporting

As a service provider, OASH must continuously provide documented, reasonable assurance that the CCP system has adequate controls and safeguards in place. Results shall be used in the audit of the HHS-wide financial statements and relied upon by other firms in examining operating division financial statements.

12 System Generated Reports and Reporting Tool Functionality Requirements

The offered system shall provide reporting tools and utilities that allow the FSB Payroll Technicians and expert users within the internal Payments and Accounting Team, to validate calculations, outputs, and payments as they process payroll each month. The reporting tools and utilities shall provide unencumbered access to PHS pay and personnel data, system and individual parameters, transactions, workflow events, calculations, and

tables, on a 24 by 7 basis throughout the year. Specifically, the following services are required:

12.1 Ad-hoc Reporting Tool

While each payroll calculation is verified by the originator and a reviewer before the final processing of any transaction, variance reports are desired as a method to identify changes in payroll from period to period and to identify the reasons for the changes. To validate the functionality of the proposed system, the ad hoc reporting utility shall allow expert users to seek and identify errors in payroll processing before the completion of payroll each period. As thousands of calculations occur each month, mistakes shall most certainly be made, but AOS has an obligation to provide accurate results before payroll is released.

The need for ad hoc reporting extends further as well. There are many requests for information from management, auditors, one-time questions, and report requests resulting from problems identified in reconciliation.

12.2 Payroll Processing

Payroll processing is typically conducted in two stages: a preliminary run is performed mid-month and payroll is finalized at the end of the month. Thus, FSB requires that at any time in the pay period, a System Administrator or Payroll Supervisor may initiate a process that will lock the payroll of all changes, calculate a draft of final pay, and create a set of payroll reports that are available online for detailed review.

Later in the month, the final pay process shall be initiated, allowing the System Administrator or Payroll Supervisor to review the status for all payees, including all earnings, deductions, taxes, and net payments, before initiating final disbursement through the Department of Treasury.

13 Post Payroll Processing Requirements

13.1 Post Payroll Processing (PACT)

The offered solution will continue to provide a set of reports formatted in accordance with the requirements of the Payments and Accounting Team (PACT) of the Commissioned Corps Systems Branch. PACT provides payroll accounting, certification, and reporting services for the Commissioned Corps Systems Branch. No less than 33 reports are produced post payroll for PACT and downstream clients of the Commissioned Corps.

13.2 Accounting for Pay System (AFPS)

The offered solution will continue to also provide a set of master reports formatted in accordance with the requirements of the Financial Management Service (FMS). FMS maintains the Accounting for Pay System (AFPS) interface, which provides Department-wide payroll accounting services for HHS civilian employees and Commissioned Corps Officers. For the Corps, AFPS is also responsible for:

- Payroll accounting for disbursements, obligations, and accruals for personnel costs.
- Collection and disbursement of payroll income taxes and reporting of those items to the Treasury Department, 50 States, the Internal Revenue Service, and the U.S. Department of Labor

The offered solution will continue to also provide budgetary/expense reporting such that CCHQ leadership, its branches track and engage with business intelligence as it related to personnel costs. The offered solution will continue to include budgetary analytics formatted for the budget office as well as each Branch to include the Ready Reserve component of the Commissioned Corps.

13.3 Continuation of Operations Requirements

13.3.1 Congressional Mandates & Mandatory Changes

From time to time, the United States Congress or other branches of the U.S. Government will issue legal mandates or mandatory changes that must be implemented or applied by the United States Public Health Service. In these events, the offeror will be required to discuss and modify its software application to implement the required modification(s).

13.3.2 Backup/Replication

The offeror shall detail the process and procedure for the daily replication, incremental and full system backup of employee and payroll data. Consideration shall be given to system availability and security requirements.

13.3.3 Service Redundancy

The offeror shall identify which components of its system are redundant, clustered, and single- point-of-failure. We define these terms as:

- Redundant – failure of this unit will cause no loss of service or performance
- Clustered – these items share the full load. When failure to one item occurs; the system shall continue operating with the remaining units, but at a reduced performance level.

- Single-point-of-failure – means discontinuation of service and potential activation if this item fails

13.3.4 Test Site

PHS also desires a Test Site to provide an environment whereby PHS may A) validate new releases before production deployment, and B) test any transaction before execution of that scenario on the new consolidated production system. To perform these functions the PHS Test Site shall be maintained by PHS personnel to be kept in daily synchronization with the executable software on the CCP Production server. PHS personnel shall also ensure that the PHS Test Site is kept in monthly or weekly synchronization with the primary CCP production database. When necessary, the PHS operators shall be required to remove the Test Site from operation to enable the Cold Site.

-

13.3.5 Devolution Planning

The Vendor shall participate in the devolution planning including identifying systems and the transfer of responsibility for the performance of essential functions to personnel at an alternate location that offers a safe and secure environment in which essential functions can continue in the event of an emergency

13.3.6 Software License

The Government wishes to purchase a perpetual license of the software from the Contactor to allow the U.S. Public Health Service to continue to process payroll in the event of a catastrophic and unforeseen circumstance regarding its supplier. The Supplier must be willing to sign a License Agreement supporting the Government's right to purchase and modify the software for its internal usage when producing Commissioned Corps payroll.

13.3.7 Documentation and Training

The vendor will complete the training and operation manuals, as well as provide training to educate the Production, Cold Site and Test Operators. The documentation and training will be structured to allow the Government to run Mock Payrolls with guidance and limited support from the vendor.

The training will be provided in Option Period 2 only. The vendor will deliver comprehensive documentation and substantial training to any number of Government personnel. There is no limit to the number of Government staff the vendor will training in a single, consecutive day session. Please be

prepared for no less than 3 days of training to allow the Government to operate in subsequent years. Also, the documentation, will be constructed such that support from vender could be reduced.

13.3.8 Automation

The Contractor will provide End to End Process Automation

- Provide capability to add additional/supporting documentation to the NOA processing modules. The supporting document should be combined to the PO created by the NOA. Meta data file should be created for automated input to the eOPF system.
- The Contractor will provide XMASTER automation
- Process xmaster based on a schedule and SFTP the files to CCMIS server.
- The Contractor will integrate the Payroll and Leave site with Access Management System (AMS) and CCMIS for single sign on.
- CCMIS secure area is authenticated using AMS. AMS already has the current officer information, as well as the CCHQ users.

14 User Roles, Accounts and Related Functions Requirements

Within the offered system, access of registered users to specific data elements, system transactions, information views and other user functionality shall be assigned on a role-by-role basis by the System Administrator. Users may be assigned to more than one role at any given time. In addition to HR Specialist and Payroll Technician, please include these two roles:

14.1 Liaison Officers

Commissioned Corps officers are assigned to a variety of positions throughout the U.S. Department of Health and Human Services (HHS) and certain non-HHS Federal agencies and programs. The Liaison Officer's role is to serve as the point of contact for assisting and coordinating activities between the Corps and a particular agencies or program. The offered solution will continue to allow Liaison officers to view data changes, transactions and personnel records of officers assigned to their agency or program.

14.2 Self Service

The offered system shall include a self-service module that will allow Officers significant control of the distribution of their gross pay (W-4, state tax, allotments, net check to bank, etc.), and online access to view, print and manage personal information at any time.

15 Year End Processing Requirements

15.1 W-2/1099/1095 Processing

In January of each year, the offeror shall print/mail W-2 statements to each Active Duty Officer and 1099R statements to each Retired Officer, Former Spouse and Annuitant paid in the prior calendar year in accordance with IRS regulations on behalf of the Commissioned Corps. The offeror shall also prepare and submit W-3 statements to the IRS and prepare/submit equivalent statements to each State tax office (as required). W-2/1099R statements shall be available for viewing, saving, and printing to all payees via a web-based self-service capability inherent in the solution.

At the same time, the offeror will print/mail 1095 statements to each Active Duty Officer and in accordance with IRS regulations regarding the Affordable Care Act. The offeror will also prepare and submit 1094 statements to the IRS (as required).

15.2 Monitoring and Quality Control

All work under this contract shall be monitored by the Contracting Officer Representative (COR), who will serve as the primary technical representative for the Government. In addition, work efforts performed in support of this SOW require senior-level management oversight, control and direction in communications, risk management, cost management, system changes/development, and quality assurance and quality control.

To keep senior-level management and the primary staff up to date on the quality of support provided, the vendor shall:

- Coordinate with the COR to provide quarterly updates to the Director of CCHQ on services provided in support of the functions to be performed;
- Participate in in-progress review meetings as required with the COR and staff;
- Monitor and maintain all existing business applications and correct defects as they become known;
- Effectively address approved system changes and changes in work priorities; Ensure proper staffing and skill set coverage at all times;
- Ensure compliance with all Government/HHS/OASH 508 compliance regulations.

16 Special Pays Requirements

The vendor will continue the functions required to support and conduct the following: Health Professions Special Pay (HPSP) – Incentive Pay (IP), Board Certified Incentive Pay (BCIP), Retention Bonus (RB), Accession Bonus (AB), and Critical Skills Wartime Accession Bonus (CSWAB), and Assignment Pay (AP). The special pay categories include these items:

- Modification and maintenance of database tables to hold the regulated contract values of the of the HPSP and AP Special Pay
- DOEs added to the database to store the calculated amounts of each new Special Pay,
- Creation of new or modification of existing NoAs to collect, modify and potentially remove the contract terms for the HPSP and AP Special Pays.
- Changes to the display to show the Special Pay contract amounts and the calculated payment values of the Special Pays on a one-time or monthly basis as required by the specification.
- Necessary modifications to the calculation engine to support the one-time or month to month calculation of the Special Pays
- Necessary modifications to the calculation engine to support the proper taxation of the new categories of Special Pay
- Modification of the xMaster interface file to support reporting of the five new categories of Special Pays
- Testing of each new category of Special Pay to ensure input, modification and possible deletion of contract terms are handled as the government expects, plus testing of the calculation engine to ensure Officers will receive the proper amounts on their Earnings/Leave Statements
- Regression testing to ensure that the existing operation of the CCP/Payroll HR/ System is not impacted by the deployment of these new categories of Special Pays.
- Develop reporting tools to administer and track Special Pays, validate Special Pay payroll updates, and monitor for transactions that impact officer's eligibility for Special Pays.

17 Work Plan/Timeline Requirements

Changes to the Special Pays will include in the work plan and timeline:

- Functional Specification
- Definition of Test Cases:
- Software Development
- Testing & Validation
- Production Release
- Ongoing error resolution

18 External Interfaces to the Current Payroll Environment

Agency	Data	Frequency	Source	Comments
DHHS	New Hires: Call to Active Duty (CAD)	Continuous	ORACLE	Import of CAD information
	Personnel Transaction Data	Continuous	ORACLE	Export of personnel data
SSA	New Hires	Monthly	CCP	Plus error feedback
	Wages	Quarterly	CCP	Plus error feedback
Treasury	Active/Retired paper check	Monthly	CCP	
	Active/Retired EFT salary	Monthly	CCP	
	Active/Retired third party payments	Monthly	CCP	Paper checks, CCD+, & CTX
	Cancelled payments	Continuous	Treasury	Daily pick-up

	Change of Account notification	Continuous	Treasury	Daily pick-up
	Financial Organizations	Monthly	Treasury	Update pick list
VA	Awards: new/changes	Continuous	VA	Mainframe drop-off
Federal Reserve	US Savings Bonds	Monthly	CCP	Pittsburgh
Thrift Savings	Contributions and personal data	Monthly	CCP	
	EDTS feedback	Continuous	TSP	Data and error feedback
	Adjustments	As Needed	PC	Web-based system
DMDC	Active personnel	Monthly	CCP	
	Active finance	Monthly	CCP	
	Active transactions	Monthly	Wang	Adds/drops/etc.
	Retired pay	Monthly	CCP	
	Survivor pay	Monthly	CCP	
	Former Spouse pay	Monthly	CCP	
	BAH population	Monthly	CCP	
	Overseas Housing	Monthly	CCP	Expenditures
	CONUS COLA	Monthly	CCP	Expenditures
	PHS DEERS Extract	Monthly	DMDC	Reconciliation
	OHA rates	Bi-Monthly	DMDC	Mainframe import
	BAH rates	Yearly	DMDC	Mainframe import
	Zip to MHA table	Yearly	DMDC	Mainframe import
	CONUS COLA rates	Yearly	DMDC	Mainframe import
Vendor Allotments	Active-Duty Dental	Monthly	CCP	1 input; 2 feedback
	Retired Dental	Monthly	CCP	1 input; 2 feedback
	Active long-term care	Monthly	CCP	1 input; 2 feedback
	Retired long term care	Monthly	CCP	1 input; 2 feedback
	Tricare Prime	Monthly	CCP	1 input; 2 feedback to three
Tax Information	W-2 (electronic)	Yearly	CCP	IRS/SSA/40+ States
	1099-R (electronic)	Yearly	CCP	IRS/30+ States
	W-2/1099-R (paper)	Yearly	CCP	All other states
DHHS Reporting	Umbrella Accounting	Monthly	CCP	Eight (8) files
	Personnel Data (PDR)	Monthly	CCP	Strength count
	Federal Tax	Quarterly	CCP	
	State Tax	Monthly	CCP	
	Payroll General Ledger	Monthly	CCP	
	PDR Sub-files	Monthly	CCP	BOP/NIH/CDC/FDA
	CAN Changes	Monthly	NIH	Mainframe import

19 Ready Reserve (OPTIONAL CLIN/TASK)

CCHQ seeks to originate Ready Reserve Pay (RRPay). RRPAY is a name given to a set of functions that integrate within the payroll system, to manage personnel and payroll solution for the Ready Reserve Corps. RRPAY is not a standalone system; it represents a set of traditional and expanded functions that will be processed by traditional and additional PHSPay users.

The vendor shall expand upon the consolidated solution for the CCP system to include RRPAY. RRPAY must be capable of handling the processing of source documents, determination of all pay categories, gross-to-net calculations, and construction of interface files to communicate pay data to the various 3rd party systems required to ensure the accurate disbursement of funds. Once successfully implemented, RRPAY must be kept current, both for routine pay table adjustments and for changes to pay calculations as

mandated by the Secretary of DHHS or Congress. The vendor is expected to draw on their established methods, best business practices, and Government/industry experience in implementing the required functions.

19.1 Personnel Actions

The RRPay system will support a full range of personnel actions from appointment and call to duty through termination or retirement. RRPay should allow Ready Reserve officers to be called to continuous active duty within eligible parameters as specified within CCD121.07§6-6. The following personnel actions (NoAs – Nature of Actions) need to be written and deployed for use in the CCP system:

Table 1 Require System Data Outputs

System Output	PURPOSE
Reserve Appointment	Appointment to Ready Reserve
Reserve Obligation	Capture type of reserve duty (SELRES, IRR, Standby), an obligation and reserve year are established.
Call to Active Duty	Call to Active Duty for Training/Other Tours
Transfers	Capture officer movements (changing units/obligations)
Termination	Terminate Reservists from Individual Ready Reserve, Selective Reserve or Active Reserve
Retirement	NoA allowing Reservists to retire after 20 years of reserve commitment, and allow Reservist to retire on disability

19.2 Time & Attendance

Ready Reserve Officers are assigned a Unit when appointed to the Ready Reserve Corps. Officers should automatically be given online self-service access to RRPay to capture and track their days worked. RRPay will record and make available the number of days of training by the Reservist in each month. Further, RRPay will allow for the Reservist to review and assert attendance at each scheduled training session.

19.3 Ready Reserve Budget/Expense Reporting

The offered solution will continue to provide a set of master reports formatted in accordance with the requirements of the Financial Management Service (FMS). FMS maintains the Accounting for Pay System (AFPS) interface, which provides Department-wide payroll accounting services for HHS civilian employees and Commissioned Corps Officers. For the Commissioned Corps, the Financial Services Branch (FSB) is responsible for: Payroll accounting for disbursements, obligations,

and accruals for personnel costs; collection and disbursement of payroll income taxes; and, reporting of those items to the Treasury Department, 50 States, the Internal Revenue Service, and the U.S. Department of Labor.

The offered solution will continue to also provide budgetary/expense reporting such that CCHQ leadership, its branches track and engage with business intelligence as it related to personnel costs. The offered solution will continue to include budgetary analytics formatted for the budget office as well as each Branch.

These functions are required to be deployed to support the Reserve Corps officers:

SYSTEM DATA OUTPUT	PURPOSE
My Schedule	View drilling schedule, unit/team, and location
My Attendance	View my attendance at scheduled drilling location
My Time	Track/Record an officer's work, training, and inactive time
Accrue Leave	Accrue annual leave for officers while on active duty
Request Leave	Allow leave requests while on active duty
My Points	View retirement points (service credit) report
My RRPAY	Compensate an officer for time worked

19.4 Unit Command

Unit Commanders must be enabled to set schedules, review, and approve officer attendance. RRPAY will also display accurate monthly information for Regional Command to validate time worked this period for Reservists.

SYSTEM DATA OUTPUT	PURPOSE
Attendance approval	Allowing Unit Command to review/approve Reservist's weekly time
Certify Monthly Time	Unit Commanders certify monthly attendance (for payroll)
Drilling counter	Track the drilling days accumulated each year
Drilling report	Display schedule showing days planned/trained each year
Historical report	Display attendance for particular dates

19.5 Ready Reserve Payroll

Each pay period begins on the first day of each calendar month with officers being paid on a 30-day month schedule. In some years, officers are paid twice in December

on the first and last workday of the month. Pay day for Ready Reserve officers is the first day of the following month, or the previous business day, if the first day of the month is not a business day.

For example, when Ready Reserve officers work in September, either drilling or active reserve, their time will need to be recorded, preferably in September. Later, in October, time worked must approved and validated. Payment will be made either the first business day of November or the last business day of October.

Payroll processing is typically conducted in at least two stages: a review by RR Command of time worked last month. Once time worked is approved, FSB may initiate a process that will lock the payroll of all changes, calculate a draft of final pay, and create a set of payroll reports that is available for detailed analysis.

Late in the month, the final pay process shall be initiated, allowing the Payroll Administrator or Payroll Supervisor to review the status for all payees, including all earnings, deductions, taxes, and net payments, before initiating final disbursement through the Department of Treasury.

19.6 Payroll Calculation Engine

The payroll engine shall calculate Ready Reserve pay based on time worked. Time worked may be inactive training, active training, or active duty.

Once time worked is tallied into a gross amount, the RRPAY solution should calculate pay for Ready Reserve Corps officers in a manner consistent with Regular Corps. In accordance with CCD121.07§7-2, payroll calculations for the Ready Reserve Corps shall reflect the military pay, entitlements and allowances for organizational structure, appointments, calls to active duty, capabilities and training, service commitments, special and incentive pays, separations and terminations.

The payroll engine shall support pay rules for the Ready Reserve, including payee classes, wage tables, source to net calculations and post-tax computations. In accordance with Congressional mandates, rules may be added, removed, or amended to fit changing criteria within the Corps.

Pay rules shall support Special Pays as applied to the various categories of Officers, including Medical, Dental, and other Special Pays.

SYSTEM DATA OUTPUT	PURPOSE
Payroll calendar	New payroll calendar tied to the Active-Duty calendar
Payroll calculator	Payroll calculator capable of determining compensation for active drilling, annual training, and Active Reserve time

SYSTEM DATA OUTPUT	PURPOSE
Payroll review	Tools to validate, certify and close the Reserve payroll

19.7 Retirement credit tracking

The Service Credit Calculator and Statement of Service report will be reviewed and modified to account for Ready Reserve requirements, including the accumulation of points towards retirement.

19.8 Leave accrual tracking

Leave and absence tracking shall be fully integrated in the RRPAY system. Leave accounting and management of leave shall be implemented as per the policies and procedures related to annual leave for Ready Reserve officers as per the Reserve Corps leave policy as described in: <http://dcp.psc.gov/ccmis/ccis/documents/CC362.01.pdf>. Additionally, an on-line leave and earnings statement will be available for viewing and printing by the Ready Reserve officers through their self-service accounts.

The RRPAY system should allow HR Specialists and regional Unit Commanders to enter and manage the necessary documentation for, and produce reports on, Leave and Absence for each Reservist.

19.9 Officer profiles

RRPAY will be system of record for officer attributes, including SERNO, drilling station, pay scale and other special pay information. Regional Commanders will be allowed to view, while HR Specialists will be allowed to enter, update, and view all officer-specific personnel information. The functionality must include storage of necessary documentation for, and producing reports on, each Ready Reserve officer who is required to have a profile.

19.10 Electronic 3rd party interfaces

The payroll/personnel component and leave component of the RRPAY system must transmit/receive data to each other. Additionally, RRPAY may have interfaces to numerous internal and external data systems, including COPPS, DEERS, TSP, VA, etc. In addition, data in the RRPAY system must accept inputs from and deliver exports to CCHQ human resource applications. These include the database tables supporting the applicant application, the promotion application, the officer evaluation application, and the electronic officer personnel file (eOPF) system.

SYSTEM DATA OUTPUT	PURPOSE
Retirement Credit	Track points and inactive time
Leave Tracking	Accrue/Use only when Active
Officer Profile	Modify to display only ready reserve information
Retirement	Support reserve, non-regular retirement
3rd party interfaces	Establish and maintain bi-directional connection from payroll/personnel to leave systems

19.11 Regional Operations

Reservists are organized geographically, each reporting to a Regional Command. Each Regional Command will consist of Operations, Administration, Budgeting and Support. Further, the solution must display historical reporting to demonstrate trends in each area of Command's responsibility: Operations, Administration, Budgeting and Support. RRPAY should enable Operations and regional command to record, designate and change primary and backup locations for drilling assignments. RRPAY should allow Ready Reserve officers to be assigned and scheduled to applicable locations for their drilling obligation of 1 weekend per month and at least 15 days active duty per year, or equivalent. The offered solution will continue to provide scheduling, assignments, and attendance recording.

SYSTEM DATA OUTPUT	PURPOSE
Drilling location	Capture information on each of the drilling locations within each of the geographic regions
Drilling assignments	Assign/change drilling location(s) and teams within a unit
Drilling schedule	Display monthly drilling schedule showing planned dates, and allow Reservists to be assigned a date and location
Drilling dashboard	Display drilling schedule showing Reservists trained and paid each month
Drilling Report	Historical report displaying attendance for particular dates

19.12 Attendance Actions

The RRPAY system will support a full attendance function from scheduling and orders to attend to approval and certification. RRPAY should allow Ready Reserve Commanders and Unit Administrators to schedule drills (UTAs) and Order Reservists to attend. The following attendance functions need to be written, tested,

and deployed for use within the offered solution:

Step	Name	Responsible User Role	Description of Standard Attendance Processing
Obligation			
1	Drill Order	CCHQ/RR Director	CCHQ/RR Director approves regions to conduct drills for a year
2	Set Schedule	Unit Command	Individual regions create a proposed schedule with drill dates
3	Attendance Order	Unit Operations	Eligible Reservists are ordered to attend the drilling session
4	Receive Orders	Reservist	Each Individual Reservists receive orders for each drill
5	Attend Drill	Reservist	Individual Reservists attends drill session as ordered
6	Take Attendance	Unit Operations	Unit Operations record Reservists who attended each drilling session
7	Approve	Unit Command	Unit Command approves the recorded attendance, then
8	Certify	CCHQ/RR Director	The CCHQ/RR Director certifies all regions who approved attendance

19.13 Payroll Actions

Beginning March 2021, Reservists will be paid and will receive points for drilling and other work. RR Officers will be paid for Inactive Duty for Training (UTA), Active-Duty Training and deployments to Active Duty. Reservists will earn Base Pay, receive BAH/BAS entitlements and some officers are eligible for Special Pays. The offered solution system must be enhanced to support all the calculations necessary to achieve accurate pay for every Reservists, regardless of their work schedule.

19.14 Reporting Actions

The RRPAY system will support reports that depict all activities performed and pay received by Ready Reserve Officers. Reservists, Regional Units and CCHQ users will have reports that include drills attended, deployments and all activity for an officer. These reports will be added to the CCP system to show pay for all activities of the Ready Reserve Corps.

20 Program Management Requirements

The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture, and CCHQ Configuration Management requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC framework and methodology and be in accordance with the HHS Contract Closeout Guide (2012). In addition, the Contractor shall develop and implement a Program Management Plan (PMP) that includes the management and oversight of all

activities performed by Contractor personnel, including the effective use of subcontractors to satisfy the objectives and service level requirements identified in this contract. The PMP will be reviewed and receive final approval from the CCHQ COR and CCHQ Business Owner Designee.

The PMP shall include:

- Methods for managing key elements of the technical approach, resources, communication, assumptions, risk, and schedule
- Strategies for managing component level activities, deliverables, critical dependencies, and milestones; and
- Description of the data to be collected to support service level and performance management and how often that data will be collected.
- Comprehensive breakdown of how delivery oversight, program management, and planning will be completed; and
- How the Contractor will accomplish through-service-level management and metrics analysis for each of the objectives presented.
- The Contractor shall provide PMP updates annually, following exercise of optional services that require operations and maintenance services, or as changes are required. The Contractor shall exercise management and operational control and assume full responsibility for all Service Levels Objectives.

21 Transition Services and Transition Plan Requirements

The Contractor shall also have all service management resources and support services in place and in full compliance with the operational requirements of the contract. The transition will be transparent and seamless to the users with no degradation or breaks in service availability while maintaining existing security, service quality, contract support, performance levels, and an orderly transition of assets. The contractor shall develop a Transition-In Plan to transition from the current IT contractor within 60 days. The Contractor shall submit a transition plan that details the methods that will be used to ensure a smooth transition from the incumbent Contractor's operation to sole operation by the new awardee. At a minimum, the Transition Management Plan (TMP) shall include:

- A milestone chart detailing timelines and stages of transition from the effective date of BPA performance until the Contractor assumes sole responsibility for providing services.
- An organizational chart that displays internal and external organizational relationships. The organizational chart shall identify the individuals by name (at all levels) who will be responsible for the transition and their respective roles; detail the lines of communication and how the Contractor will interface with HHS during this phase of BPA performance.
- Written documentation of technology and data systems, as well as a written plan for making access to these systems available for new hires.
- Define the Scope of the Data Transfer and Migration Process: Specify the systems, databases, applications, and datasets involved in the data transfer and migration process.

- Specify Requirements for Data Mapping, Analysis, and Validation: Define requirements for data mapping, analysis, and validation to ensure the accurate transfer of data from the incumbent vendor's system to the new service provider infrastructure.
- Address Data Security and Privacy Considerations: Include encryption protocols, access controls, compliance with regulatory requirements, and measures to protect sensitive information during transit and storage.
- Outline Procedures for Extracting Data: Detail procedures for extracting data from the incumbent vendor's system, transforming it into the required format for migration, and verifying data integrity throughout the process.
- Data Migration and Transfer Methodology: Describe the methodology for data migration and transfer, including the approach, tools, and techniques utilized.
- Data Migration Testing: Define the testing procedures for data migration to ensure accuracy, completeness, and integrity of transferred data.
- Methods to orient and educate incumbents/new hires about the Contractor's HHS' processes.
- Plans to communicate and cooperate with the current incumbent Contractor.

Transition activities include the transfer of privileged account passwords, proper documentation of all IT assets, and the issuance of Government-Furnished Equipment (GFE).

21.1.1 Transition-In shall be deemed complete as of the first business day following the Service Acceptance Date as specified in the TMP. The Government will confirm acceptance with a written notice accepting implementation and deployment of all required TMP activities to CCHQ's satisfaction specified in this contract. The exact time and location will be determined at time of the contract award. This meeting will be at no charge to the Government.

21.1.2 Attend a post-award kickoff meeting

The Contractor shall participate in a post-award kickoff and introduction meeting with CCHQ representatives within 14 calendar days after TO award in the Washington DC area. The contractor will be required to provide a presentation introducing its team members to CCHQ and to give a brief synopsis of the team's capabilities. The exact time and location will be determined at time of the TO award. This meeting will be at no charge to the Government.

21.2 Transition-Out Period and Plan

The contractor shall develop and implement a Transition-Out Plan to detail the process for an orderly transition of work to a successor Contractor. The transition is to be transparent and seamless to the users with no breaks in service availability while maintaining existing security, service quality, contract support, performance levels, and an orderly transition of assets. CCHQ expects transition-out tasks to be coordinated, integrated, and initiated with the successor Contractor transition-in tasks prior to the end of the period of performance and with enough time to meet the stated

objective. Upon completing transition-out activities, the Contractor will transfer all GFE back to the Government.

The contractor shall provide a Transition Out Plan. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor /government personnel at the expiration of the contract. The contractor shall provide a Transition-Out Plan NLT ninety (90) calendar days prior to expiration of the contract. The contractor shall identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following:

1. Project management processes.
2. Points of contact.
3. Location of technical and project management documentation.
4. Status of ongoing technical initiatives.
5. Appropriate contractor to contractor coordination to ensure a seamless transition.
6. Transition of Key Personnel.
7. Identify schedules and milestones.
8. Identify actions required of the Government.
9. Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via status meetings.
10. Transfer of OASH/CCHQ data within the current system
11. Transfer of applicable all materials and supplies that are the property of the Government or purchased, throughout the life of the Contract, on behalf of the Government.
12. Applicable materials shall be provided in the most appropriate format, as agreed upon by the parties

The Contractor shall plan for and provide a transition-out period not to exceed 60 days.. At a minimum, transition out services shall include the following:

- Developing a transition-out plan for transferring service responsibility from this award to another provider or back to CCHQ. The transition plan shall identify tasks/requirements needed to ensure the successful transfer all responsibilities to another party.
- Known risks, foreseeable problems, and shall identify the additional resources and cost, if any, required to mitigate these risks and ensure a successful transfer of responsibility.
- Delivering to CCHQ all agency related account, inventory, invoice, and other data resident in the Contractor's data system necessary to enable another provider, to assume service responsibility. This information shall include all information that the Contractor works with to manage the agency's accounts, service delivery, and equipment.
- All data shall be delivered, available, and accessible to CCHQ in electronic format to enable electronic transfer into other data systems. The specific format(s) for the data will be specified during transition. This information will be referred to as Agency Transition Data.

Upon expiration of the contract, as part of its close-out responsibilities within FAR Part 4.8, the Contractor shall continue to support CCHQ and its Components in handling and tracking disputes on or before the contract expiration date through final resolution, or for six (6) months after expiration, whichever is less. (These are not contract claims as defined in FAR Part 33, which will be handled by a warranted CO.)

22 Information Security and/or Physical Access Security Requirements

22.1 Baseline Security Requirements

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

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

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

22.1.2 Safeguarding Information and Information Systems. All government information and information systems must be protected in accordance with HHS/OS policies and level of risk.

22.1.2.1 At a minimum, the Contractor (and/or any subcontractor) must protect the:

- 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.

22.1.2.2 Categorize all information owned and/or collected/managed on behalf of HHS/OS and information systems that store, process, and/or transmit HHS information 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. Based on information provided by the ISSO, CISO, OpDiv SOP, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:

- Confidentiality: ☐ Low ☒ Moderate ☐ High
- Integrity: ☐ Low ☒ Moderate ☐ High
- Availability: ☐ Low ☒ Moderate ☐ High
- Overall Impact Level: ☐ Low ☒ Moderate ☐ High

22.1.2.3 Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of HHS/OS regardless of location or purpose.

22.1.2.4 Report any discovered or unanticipated threats or hazards by either the agency or Contractor, or if existing safeguards have ceased to function immediately after discovery, within one (1) hour or less, to the government representative(s).

22.1.2.5 Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/OS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain all applicable security and privacy policies by contacting the CO/COR or HHS/OS security and/or privacy officials.

22.1.3 Privacy Act. Comply with the Privacy Act requirements (when applicable), and tailored FAR and HHSAR clauses as needed.

22.1.4 Privacy Compliance. Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/OS privacy policies, and complete all the requirements below:

22.1.4.1 Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: Social Security number, date and place of birth, mother's maiden name, biometric records, etc.

22.1.4.2 To ensure that the public's personal information is protected in a manner commensurate with the privacy risks, HHS uses a privacy analysis process to assess the risks associated with HHS's collection and maintenance of PII and to ensure information is handled in accordance

with applicable legal, regulatory, and policy requirements. PTAs analyze how information is handled in IT systems and electronic information collections and determines if the IT system or electronic information collection collects, disseminates, maintains, or disposes of PII. PIAs are used to assess the privacy risks of IT systems and electronic information collections that collect, disseminate, maintain, or dispose of PII about members of the public. PIAs also provide transparency into how HHS collects, disseminates, maintains, or disposes of the public's PII.

22.1.4.3 The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not PII is collected, disseminated, maintained, or disposed as part of the contract. The PTA will determine if a full Privacy Impact Assessment (PIA) needs to be completed.

If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within 01 July 2022-30 June 2023 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*.

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

22.1.5 Controlled Unclassified Information (CUI). Executive Order 13556 defines CUI 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, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

- Marked appropriately;
- Disclosed to authorized personnel on a Need-To-Know basis;

- Protected in accordance with NIST SP 800-53, Security and Privacy Controls for 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
- Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

22.1.6 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) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

22.1.7 Confidentiality and Nondisclosure of Information. Any information provided to the Contractor (and/or any subcontractor) by HHS or collected by the Contractor on behalf of HHS must be used only for the purpose of carrying out the provisions of this contract and must 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 must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must 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 must be protected in accordance with HHS and *OASH/CCHQ* policies. Unauthorized disclosure of information will be subject to the HHS/OS sanction policies and/or governed by the following laws and regulations:

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

22.1.8 Internet Protocol Version 6 (IPv6). All procurements using Internet Protocol must comply with OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6) available at <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf>

22.1.9 Information and Communications Technology (ICT). ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The Contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.

22.1.10 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 must 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, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.

22.1.11 Contract Documentation. The Contractor must use provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate.

22.1.11.1 Authentication RA Template, March 2019. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/guides-forms-templates>.

22.1.11.2 HHS Cloud Computing and Federal Risk and Authorization Management Program [FedRAMP] Guidance, as amended. Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/policies-standards-memoranda-guides/memoranda>.

22.1.11.3 HHS Guidance for Selection of e-Authentication Assurance Levels, March 2019. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/guides-forms-templates>.

22.1.11.4 HHS Information Security and Privacy Policy (IS2P), July 30, 2014. Available at <https://intranet.hhs.gov/working-at-hhs/cybersecurity/ocio-policies>.

22.1.11.5 HHS Memorandum, Implementation of the Section 889(a)(1)(B) Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, July 29, 2020, Available at <https://intranet.hhs.gov/contracts-and-grants/acquisition/acquisition-memorandums>.

22.1.11.6 HHS Minimum Security Configuration Standards Guidance, as amended. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides>.

22.1.11.7 HHS Mobile Applications Privacy Policy. Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/ocio-policies>.

- 22.1.11.8** HHS Policy and Plan for Preparing For and Responding To a Breach of Personally Identifiable Information (PII). Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/hhs-policy-for-preparing-for-and-responding-to-a-pii-breach>.
- 22.1.11.9** HHS Policy Exception/Risk Based Decision Request, July 10, 2019. Available at <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/guides-forms-templates>.
- 22.1.11.10** HHS Policy for Internet and Email Security, October 2019. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/policies>.
- 22.1.11.11** HHS Policy for Software Asset Management (SAM), October 2019. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/policies>.
- 22.1.11.12** HHS Policy for Software Development Secure Coding Practices, August 14, 2019. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/policies>.
- 22.1.11.13** HHS Policy for Supply Chain Risk Management. Available at: <https://intranet.hhs.gov/policy/hhs-policy-cyber-supply-chain-risk-management>.
- 22.1.11.14** HHS Policy for Vulnerability Management. Available at: <https://intranet.hhs.gov/policy/hhs-policy-vulnerability-management>.
- 22.1.11.15** HHS Rules of Behavior for Use of HHS Information and IT Resources Policy, July 25, 2018. Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/ocio-policies>.
- 22.1.11.16** HHS Standard for Encryption of Computing Devices and Information, as amended. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides>.
- 22.1.11.17** HHS Standard for Plan of Action and Milestones, as amended. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides>.
- 22.1.11.18** Policy for Information Technology (IT) Enterprise Performance Life Cycle [EPLC]. Available at: <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/policy-for-information-technology-enterprise-performance.html>.
- 22.1.11.19** Policy for Privacy Impact Assessments. Available at: <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/policy-for-privacy-impact-assessments.html>.
- 22.1.11.20** Requirements for Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum, as amended. Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/policies-standards-memoranda-guides/memoranda>.
- 22.1.11.21** Sensitive PII Definition and Guidance - INFORMATION, December 4, 2018. Available at: <https://intranet.hhs.gov/technical-support/cybersecurity/policies-standards-memoranda-guides/memoranda>.

22.1.11.22 HHS Cybersecurity Program Available at:

<https://intranet.hhs.gov/working-at-hhs/cybersecurity>

22.1.11.23 Privacy Program Available at: <https://intranet.hhs.gov/working-at-hhs/cybersecurity/hhs-privacy-program>

22.1.12 HHS Section 508 Accessibility Standards

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

All products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, B, C & D, and available at <https://www.access-board.gov/ict/>.

All requirements are applicable to support services and documentation deliverables. All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

For each proposed product, platform, or service, a fully completed Accessibility Conformance Report (ACR) using the Voluntary Product Accessibility Template (VPAT) (<https://www.itic.org/policy/accessibility/vpat>) must be submitted. Evaluation will be on an Acceptable/Unacceptable basis.

Prior to acceptance of deliverables, the offeror must demonstrate conformance to the HHS Section 508 requirements via HHS Section 508 checklist(s) (<https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>). The government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance does not meet the HHS Section 508 requirements, the government shall, at its option, require the offeror to remediate the item, at no additional cost to the government, to align with the HHS Section 508 conformance requirements prior to acceptance.

References:

- Section 508 Standards: <https://www.access-board.gov/ict/>

- HHS Policy on Section 508 Compliance and Accessibility of Information and Communications Technology (ICT):
<https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/department-of-health-and-human-services-hhs-policy-on-section-508-and-accessibility-of-technology.html>
- HHS Accessibility and Section 508 Compliance Checklists:
<https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>

22.1.13 Standard for Encryption.

The Contractor (and/or any subcontractor) must:

- Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
- 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 encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
- Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OpDiv-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).
- Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR and/or designated government representative(s). 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 <http://csrc.nist.gov/publications/>. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.

22.1.14 Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the OpDiv non-disclosure agreement, as applicable. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

22.2 Training Requirements

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

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

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

22.3 Rules of Behavior

22.3.1 The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, *HHS Rules of Behavior for Privileged Users*, and any other applicable HHS IT Rules of Behavior protocols, procedures, guidelines etc. .

22.3.2 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 OpDiv Information Security Awareness Training. If the training is provided by the Contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

22.4 Incident Response

22.4.1 The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/OS IRT teams **within 24 hours**, whether the response is positive or negative. In accordance with FISMA and OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is “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” and a privacy breach is “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.” For additional information on the HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*.”

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

22.4.2.1 Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

22.4.2.2 NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, the Contractor must send *OS approved* notifications to affected individuals.

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

- Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
- Not include any sensitive information in the subject or body of any reporting e-mail; and
- Encrypt sensitive information in attachments to email, media, etc.

22.4.2.4 Comply with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and HHS and OS privacy breach response policies when handling PII breaches.

22.4.2.5 Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including

providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to Contractor facilities during a breach/incident investigation.

22.5 Position Sensitivity Designations

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

Investigation/Tier	Position Requirement/Information Sensitivity
Tier 2S WITH SUBJECT INTERVIEW	Moderate Risk Public Trust (MRPT)
Tier 4	High Risk Public Trust (HRPT)

22.6 Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1§1.2*.

22.7 Roster

The Contractor (and/or any subcontractor) must 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 must be submitted to the COR and/or CO within fifteen business days of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within 3 *business days* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

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

22.8 Contract Initiation and Expiration

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

22.8.2 System Documentation. Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

22.8.3 Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must 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*.

22.8.4 Notification. The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO within 24 hours before employees stop working under this contract.

22.8.5 Contractor Responsibilities upon Physical Completion of the Contract. The Contractor (and/or any subcontractors) must 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 must 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 *OASH CCHQ* policies.

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

22.9 Records Management and Retention

22.9.1 The Contractor (and/or any subcontractor) must 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 Policy for Records Management* and *OASH/CCHQ* policies and must not dispose of any records unless authorized by HHS/OASH.

22.9.2 In the event that a Contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS/OASH policies.

22.10 High Value Asset (HVA)

If a system is identified as HVA², the Contractor must comply with the HHS Policy

² High Value Asset (HVA)- Federal information or a Federal information system that relates to one or more of the following categories:

-Informational Value – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
-Mission Essential - The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
-Federal Civilian Enterprise Essential (FCEE) - The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise (OMB M-19-03).

for the High Value Asset (HVA) Program and the DHS HVA Control Overlay, <https://community.max.gov/display/HHS/HHS+CyberSecurity+Policy+Collaboration+Page>, in addition to the above requirements.

23 Requirements for Procurements Involving Privacy Act Records

23.1 Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals from which records are retrieved by name or other identifying particular.

The System of Records Notice that is applicable to this contract is: 09-40-1402 HHS Payroll Records.

The system of records design, development, or operation work the Contractor is to perform is: The Department of Health and Human Services (DHHS) is looking to consolidate its HR and payroll functions onto a single administrative platform. Currently, its personnel processing, personnel order management and payroll system supporting the active duty and retired Commissioned Officers of the United States Public Health Service (USPHS) are on multiple systems. The consolidated system must be able to handle the collection of source documents, determination of all pay categories, gross-to-net calculations, and interface with all the various internal and external systems required to ensure the accurate disbursement of funds and maintenance of all related IT systems. Once successfully implemented, the system needs to be kept current: both for routine pay table adjustments and for changes to pay calculations as mandated by the Secretary of DHHS or Congress. The Contractor is expected to draw on their established methods, best business practices, and Government/industry experience in applying application.

These functions will be performed on the consolidated system:

- Assignments
- Awards
- Immunizations tracking
- Leave & Absence Tracking
- Licensure tracking
- Officer profiles
- Officer self-service
- DD214/215
- Promotions
- Retirements & Separations
- Position management
- Readiness compliance
- New Hires/Call to Duty
- Adverse Actions

- Post payroll processing
- Retirement
- Active-duty payroll
- Security clearance tracking

The disposition to be made of the Privacy Act records upon completion of contract performance is: At the end of contract performance, OASH CCHQ will provide disposition instructions to the Contractor for securely transferring or destroying (in accordance with NIST SP 800-88) any agency records that are in the Contractor's (or sub-contractor's custody or control.

23.2 Procurements Involving Government Information Processed on GOCO or COCO Systems

23.2.1 Security Requirements for GOCO and COCO Resources

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

23.2.1.2 Assessment and Authorization (A&A). A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) *OS timeline(s)*. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ OS policy if any*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).

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

23.2.1.2.1 A&A Package Deliverables - The Contractor (and/or any subcontractor) must provide an A&A package within the timelines, processes and formats identified in the HHS guidance listed below. The development and completion of A&A activities and deliverables will be under the supervision of the assigned OASH System Owner and ISSO. Deliverable due dates may have to be

adjusted to accommodate the availability of government A&A resources. The Contractor shall request adjustments to deliverable due dates in writing and submitted to the CO for approval. the CO and/or COR.

- [HHS Policy for Information Security and Privacy Protection \(IS2P\)](#)
- [HHS Policy for Information Security and Privacy Protection \(IS2P Control Catalog\)](#)
- [HHS Policy for Information Technology \(IT\) Policy for Enterprise Performance Life Cycle \(EPLC\)](#)

The following A&A deliverables are required to complete the A&A package. All deliverables are to be provided in accordance with the applicable formats and guidelines listed above.

- **System Security Plan (SSP)** - Due 60 days *he* SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least *annually* thereafter and if requested, provide a copy of the updated SSP.
- **Security Assessment Plan/Report (SAP/SAR)** - assessor and be consistent with NIST SP 800-53A or latest revision, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with **OS must** assist in the assessment of the security controls and update the SAR at least *annually*. A copy of the updated SAR should be provided if requested.

- **Independent Assessment** - due 30 business days in accordance with the following HHS guidance
 - [HHS Policy for Information Security and Privacy Protection \(IS2P\)](#)
 - [HHS Policy for Information Security and Privacy Protection \(IS2P Control Catalog\)](#)
 - [HHS Policy for Information Technology \(IT\) Policy for Enterprise Performance Life Cycle \(EPLC\)](#)
- The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all "*high*" deficiencies before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).
- **POA&M** – After positive identification of scan findings or approval of security assessment/audit report, all findings/weaknesses shall be documented in a POA&M, reported to HHS, and remediated/mitigated within the following remediation timelines. Remediation refers to complete fix of a weakness; whereas, mitigation refers to remediating the weakness to an acceptable level of risk, but not fully resolved. NIST SP 800-53 defines risk mitigation as “Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.”
 - Critical within 15 days (in accordance with DHS BOD 19-02);
 - High within 30 days (in accordance with DHS BOD 19-02;)
 - Moderate within 90 days (in accordance with FedRAMP Guidance); Moderate timeline is in line with FedRAMP requirement, and
 - Low as defined by the OpDiv, not to exceed 365 days.

OpDiv System Owners (SOs), Information System Security Officers (ISSOs), and/or other POA&M stakeholders shall determine the scheduled completion date for each POA&M

within the specified remediation timelines.

POA&Ms are due from the date the weaknesses are formally identified and documented. *HHS/OASH will determine the risk rating of vulnerabilities.* Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws, and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented, and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. Depending on the severity of the risks, *OS* may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly**.

- **Contingency Plan and Contingency Plan Test** – the Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and OS policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor must update and test the Contingency Plan at least *annually*.
- **E-Authentication Questionnaire** - The Contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS policies.

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

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

23.2.1.2.4 Asset Management - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least *[insert specific timeframe]*. IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The Contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.

23.2.1.2.5 Configuration Management - Use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS/ OS/OASH CISO monthly. The Contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

23.2.1.2.6 Vulnerability Management - Contractors must actively manage system vulnerabilities using automated tools and

technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The Contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least to HHS//OASH CISO monthly

Patching and Vulnerability Remediation - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes as outlined in the OS Patch and Vulnerability Management Processes for Operating Systems and Applications (see below).

Security-Operations / ITIO Staff members will upon receipt of the Security Center vulnerability analysis are responsible for remediating all identified vulnerabilities within the appropriate timeframe based on the risk rating of the vulnerability. Vulnerabilities that have not been remediated within the appropriate timeframe will be escalated to executive management.

Vulnerability Remediation Table

Risk Rating	Remediation Timeframe	CVSS Rating
Critical	7 Days	CVSS score = 10
High	14 Days	CVSS score > 7.5
Medium	30 Days	CVSS score between 5.0 and 7.5
Low	As capacity permits	CVSS < 5.0

Note: Timeframes are in calendar days.

In situations where critical patches are required to mitigate immediate operational risks and/or service disruptions, patches may require commensurately shorter remediation timeframes. For more information about CVSS scores please see: <http://nvd.nist.gov/cvss.cfm>.

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

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

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

23.2.1.3.1 At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours Contractor local time, to access Contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and

compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

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

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

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

23.2.1.5 Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor. The Contractor (and/or any subcontractor) must ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in

accordance with approved security configurations and meet the following minimum requirements:

- 23.2.1.5.1** Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST CMVP.
- 23.2.1.5.2** Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and HHS Minimum Security Configuration Standards;
- 23.2.1.5.3** Maintain the latest operating system patch release and anti-virus software definitions;
- 23.2.1.5.4** Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
- 23.2.1.5.5** Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
 - Using Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
- 23.2.1.6 Rights to Data, Unlimited.** The Government possesses the right to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so with any Government data and Contractor-created data during the performance period of this contract.
- 23.2.1.7 Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements.** The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with HHS Policy for Cyber Supply Chain Risk Management and Public Law 115-232 § 889. At a minimum, they must implement the following:
 - 23.2.1.7.1** Develop rules for suppliers' development methods, techniques, or practices;
 - 23.2.1.7.2** Use of secondary market components;
 - 23.2.1.7.3** Prohibit counterfeit products;

- 23.2.1.7.4 Dispose and/or retain elements such as components, data, or intellectual property securely;
- 23.2.1.7.5 Ensure adequate supply of components;
- 23.2.1.7.6 Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
- 23.2.1.7.7 Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
- 23.2.1.7.8 Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
- 23.2.1.7.9 Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
- 23.2.1.7.10 Prohibit the use of covered telecommunications and video surveillance equipment or services.

24 Contracts Involving Cloud Services

24.1 HHS FedRAMP Privacy and Security Requirements

The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:

24.1.1 FedRAMP Compliant ATO. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by the process, timelines, and formats outlined in [HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance](#)

24.1.1.1 Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.

24.1.1.2 A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and *annually* thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

24.1.2 Data Jurisdiction. The Contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS).

24.1.3 Service Level Agreements. The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with HHS/OASH to develop and maintain an SLA.

24.1.4 Interconnection Agreements/Memorandum of Agreements. The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/ *OS policies*.

24.2 Protection of Information in a Cloud Environment

24.2.1 If Contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/ *OASH* policies <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.

24.2.2 HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS within one (1) business day from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS.

24.2.3 The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

24.2.4 The Contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:

24.2.4.1 Maintenance of links between records and metadata, and

24.2.4.2 Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

24.2.5 The disposition of all HHS data must be at the written direction of HHS/OS. This may include documents returned to HHS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.

24.2.6 If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements

24.3 Assessment and Authorization (A&A) Process

24.3.1 The Contractor (and/or any subcontractor) must comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS/OASH policies *in accordance with* [HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance](#)

24.3.1.1 In addition to the FedRAMP compliant ATO, the Contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation in accordance with the requirements contained in the following HHS Policies:

- [HHS Policy for Information Security and Privacy Protection \(IS2P\)](#)
- [HHS Policy for Information Security and Privacy Protection \(IS2P\) Control Catalog](#)
- [HHS Policy for Information Technology \(IT\) Policy for Enterprise Performance Life Cycle \(EPLC\)](#)

The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.

24.3.1.2 CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

24.3.1.3 For all acquired cloud services, the A&A package must contain the following documentation:

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- POA&M
- Configuration Management Plan (CMP)
- Contingency Plan (CP) and Contingency Plan Test (CPT) Report
- E-Auth (if applicable)
- PTA/PIA (if applicable)
- Penetration Test Results
- Interconnection/Data Use/Agreements (if applicable)
- Service Level Agreement
- Authorization Letter
- Configuration Management Plan (if applicable)
- Configuration Baseline

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/OASH policies. The Contractor shall use the FedRAMP templates (<http://www.fedramp.gov/>). Deliverable

timelines will be determined by the FedRAMP guidance.

- 24.3.2** HHS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS exercises this right, the Contractor (and/or any subcontractor) must allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
- 24.3.3** The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the Contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the Contractor's expense, before HHS issues an ATO.
- 24.3.4** The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than fifteen (15) days and (2) high within thirty (30) days (3) medium within ninety (90) days and (4) low vulnerabilities no later than three hundred and sixty-five (365) days. In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines. HHS/OASH will determine the risk rating of vulnerabilities using FedRAMP baselines.
- 24.3.5** Revocation of a Cloud Service. HHS/ OS have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or OS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

24.4 Reporting and Continuous Monitoring

24.4.1 Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

24.4.2 At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis in electronic format via email or uploaded to an approved collaboration tool:

24.4.2.1 Operating system, database, Web application, and network vulnerability scan results;

24.4.2.2 Updated POA&Ms;

24.4.2.3 Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the OS System Owner or AO, and;

24.4.2.4 Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/OS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

24.5 Configuration Baseline

24.5.1 The Contractor must certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*.

24.5.2 The Contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

24.6 Incident Reporting

24.6.1 The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS OS OMB, and US-CERT requirements and obtain approval from the OpDiv. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.

24.6.2 The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS access to its facilities, installations, technical capabilities, operations, documentation,

records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:

24.6.2.1 Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/OS personnel, or agents acting on behalf of HHS/OS, using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

24.6.2.2 In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident, or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:

- Company and point of contact name;
- Contract information;
- Impact classifications/threat vector;
- Type of information compromised;
- A summary of lessons learned; and
- Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

24.7 Media Transport

24.7.1 The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards). *Physical removal and transportation of data shall be logged with documented chain of custody form and approved by the OASH CISO.*

24.7.2 All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

24.8 Boundary Protection: Trusted Internet Connections (TIC)

24.8.1 The Contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the

Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.

24.8.2 The Contractor must route all external connections through a TIC.

24.8.3 Non-Repudiation. The Contractor must provide a system that implements encryption with current FIPS 140 validation certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

25 Other IT Procurements

Information Technology Application Design, Development, or Support

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

25.2 The Contractor must consult the guidelines from NIST SP 800-160 volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST SP 800-160 volume 2, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, and NIST SP 800-53 to implement security during the development of all applications and throughout the life cycle stages of software development.

25.3 The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards, the Open Web Application Security Project (OWASP), System Admin, Audit, Network and Security (SANS), and the HHS Policy for Software Development Secure Coding Practices that will limit system software vulnerability exploits.

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

25.5 The Contractor must, at a minimum, segregate physically or logically, all test and development systems from production systems as applicable in accordance with the HHS Standard for Segregation of Dev/Test Environments from Production.

25.6 The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or

proprietary by HHS must be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

Physical Access to Government Controlled Facilities

"HHS reserves the right to exercise priorities and allocations authority with respect to this contract, to include rating this order in accordance with 45 CFR Part 101, Subpart A—Health Resources Priorities and Allocations System."

Appendix A: Service Level Agreement

This Service Level Agreement (or SLA) defines the services and the required standard for those services that a service provider will provide. This SLA is anticipated to be included as part of the Performance Work Statement (PWS) contained in HHS Contract No. TBD

The format of this SLA is:

1. Business objectives

The Office of the Assistant Secretary of Health (OASH) uses an administrative system for its population of 6,000 Commissioned Corps officers to a) process payroll, process personnel actions, manage leave and communicate data to downstream agencies and systems. The preferred solution is a cloud-based, real-time, workflow enabled offering that provides personnel and payroll processing including the electronic initiation and processing of military personnel actions, computing compensation, and maintaining personnel and payroll records for both the Active Duty and Reserve Officers of the Public Health Service. A related desire is for a leave management system that tracks the daily accrual and allows for real-time review and approval of leave requests.

Detail is provided below. Further information can be found within the Performance Work Statement of Contract No. TBD.

2. Description of the Services

Payroll transactions are processed by the staff of the Financial Services Branch (FSB), while the Separations and Assignments Branch (SAB) and the Call to Active Duty and Recruitment Branch (CADRe) process personnel transactions. Deployment orders are processed by the Readiness and Deployments Branch (RDB) while Leave and Long-term Training transactions are administered by the Personnel and Career Management Branch (PCMB). The Contractor shall manage, operate, and maintain the Government's backup services for applications and services; document the existing cloud-based functionality and data.

The following descriptions are specific to each Branch: Financial Services Branch (FSB), Separations and Assignments Branch (SAB), Call To Active Duty and Retirements (CADRe),

Readiness and Deployment Branch (RDB) Personnel and Career Management Branch (PCMB) Reserve Affairs Branch (RAB) The below applies to both active and reserve officer functions that are managed in the respective above branches.

Financial Services Branch	Military Pay & Entitlements
Complete control of payroll	Special Pays
processing, data, and business rules.	Audit & Reporting
Seamless integration with personnel	Electronic 3 rd party interfaces
order system. Intuitive setup and	Accounting & Tax Compliance
reporting tools.	Year-begin/year-end Processing
Payroll process/COOP	
Planning	Year-end training of Corps Personnel and Payroll System (CCP) and Continuity of Operations Planning (COOP) plan

Included below are detailed descriptions of each service or reference to the SOW, including what the service is, where it is to be provided, to whom it is to be provided and when it is required.

Separations and Assignments Branch	Officer and Organizational dashboards
Custom-tailored analytics,	Officer life-cycle management
authorities, experiences, roles,	Individual and Bulk Personnel Actions
responsibilities, and personnel order	Personnel Orders
workflow	Separations management
	eOPF integration

Call to Active Duty and Recruitment Branch	Appointment and Call to Active-Duty process
Custom-tailored analytics,	Prior service date calculations
authorities, experiences, roles,	Individual and Bulk Personnel Actions
responsibilities, and personnel order	Personnel Orders
workflow	eOPF Integration
	Officer life-cycle management

Readiness and Deployment Branch	Bulk or Individual Deployment Orders
Custom-tailored functions and	Mobilization Pre-orders
workflows	Demobilization Orders
	eOPF Integration

Personnel and Career Management Branch	Training Actions
Policy-driven business rules and	Leave management
position-driven communications	eOPF Integration
with electronic notifications	

Reserve Affairs Branch Complete control of pay and accountability system. Seamless integration with payroll and personnel order system. Intuitive display and clear reporting metrics and RR Financial and Force Reporting	Military Pay & Entitlements
	Special Pays
	Mandatory Unit Training Assembly (MUTA)
	Management
	Reservist and Regional dashboards
	Retirement Points Management
	Reservist Lifecycle Management

Mission Engagement, OCIO Custom-tailored functions and workflows	Secure (SOAP) Interface
	Help Desk management
	Security integration
	User management

3. Performance Standards

State the expected standards of performance for each individual service. Consider each service level carefully depending on their business importance.

Technology Infrastructure	Authority to Operate (ATO)
We require scalable technology to continuously modernize operations that support our 6,000+ officers	FedRAMP/GovCloud
	Real-time data backup/recovery
	99.45% Uptime (down for 4hrs/mo)
	Monthly security scans
	Annual SSAE Audit

The service provider and the customer will also need to set these performance standards in the context of anticipated workloads and the service levels may need to vary in the light of any changes to these workloads during the course of the Contract. The service provider will provide cost implications and/or estimates of scope changes.

4. The Contractor shall manage, operate, and maintain the Government's backup services to include supporting devolution plan for applications and services; existing cloud-based functionality and data.

5. Compensation/Service Credits.

Ensure data can be replicated and access is granted to devolution partner

Failure to achieve desired service levels has a financial consequence for the service provider, where the service provider will pay or credit the customer an agreed amount. The Contractor recommends specific formulas for calculating each service level agreement. The Contractors' maximum monthly financial risk shall be limited to 10% per month of the monthly billing for each

invoiced category.

6. Critical Failure

Include a right for the customer to terminate the agreement if service delivery becomes unacceptably bad so, the customer does not find itself in the position of having to pay (albeit at a reduced rate) for an unsatisfactory overall performance. Report any discovered or unanticipated threats or hazards by either the agency or Contractor, or if existing safeguards have ceased to function immediately after discovery, within one (1) hour or less, to the government representative(s).

7. Incident Response

- a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/ [Commissioned Corps Headquarters (CCHQ)] Director **within 24 hours**, whether the response is positive or negative. In accordance with FISMA and OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (PII), an incident is "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" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII).
- b. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
 - i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
 - ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, the Contractor must send CCHQ approved notifications to affected individuals CCHQ Specific timeline, process, and format].
 - iii. Report all suspected and confirmed information security and privacy incidents and breaches to the OASH OCIO, CCHQ Incident Response Team (IRT), COR, CO, CCHQ Standard Operating Procedure (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable CCHQ and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:

- Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
 - Not include any sensitive information in the subject or body of any reporting e-mail; and
 - Encrypt sensitive information in attachments to email, media, etc.
- iv. Comply with Office of Management and Budget OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and HHS/CCHQ and CCHQ privacy breach response policies when handling PII breaches. REF: HHS-OCIO-PIM-2020-05-003
- v. 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.

8. Incident Reporting

- a. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS OCIO, OASH OCIO, [CCHQ], OMB, and US-CERT requirements and obtain approval from the CCHQ. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
- b. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:
- i. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/[CCHQ] personnel, or agents acting on behalf of HHS/[CCHQ], using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.
 - ii. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident, or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
 - Company and point of contact name;

- Contract information;
- Impact classifications/threat vector;
- Type of information compromised;
- A summary of lessons learned; and
- Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

Section 1: System Availability

Item #	Requirements	Description	Specifications	Measurement Vehicle
1A	Availability*	<p>This metric indicates the target availability for the application and the hours designated including on-line availability for end users, batch processing capabilities and maintenance.</p> <p>The system will have full functionality and all features will be available to government users.</p>	<p>Hours of Operations: 24 hours per day except during system maintenance</p> <p>Scheduled Maintenance: Sunday and Thursday 10:00PM to 11:00 PM excluding payroll processing</p> <p>The system will be operational, consistent with the Hours of Operations as noted above. Other maintenance outages if scheduled or requested by the customer will not be measured against server system availability percentage.</p> <p>Target Availability: 99.98%</p>	<p>System Login</p> <p>Problem Alerts</p> <p>Problem Notifications</p>

** If the downtime is determined (in the Root Cause Analysis report) to be due to issues other than the application or due to the actions outside of the Contractor's control, the outage time is not included in the Availability SLA calculation*

Section 2: Operations/Problem Management

Functional Area: CCP Support	Contracted SLA
Provide continuous software Support	Monday - Friday 08:00AM - 6:00PM
Respond to email notifications during core business hours	< 60 mins
Respond to email notifications during off hours	< 8
Answer/respond to calls during core business hours	< 60 mins
Answer/respond to calls during off hours	< 8 hours
Troubleshoot issues during core business hours	< 4 hours
Troubleshoot issues during off hours	< 8 hours
Resolve/mitigate issues during core business hours	< 2 hours
Resolve/mitigate issues during off hours	< 8 hours

***Severity Levels are based on the Problem Severity Definitions below. If the Severity Level is unclear, the Division Director will make the final determination.*

Section 3: Maintenance/Application Development

Item #	Requirements	Description	Specifications	Measurement Vehicle
3A	Release Quality	This metric measures the percent of passed/failed**** test cases for Functional Quality Testing	<p><i>Enhancements:</i></p> <p><10% failure rate**** (1st iteration); <2% failure rate (2nd iteration)</p> <p><i>Maintenance:</i> <5% failure rate (1st iteration); <1% failure rate (2nd iteration)</p>	OCIO/CCHQ UAT Report
3B	Deployments	This metric measures the quality of software implementations.	<p><2 issues identified in implementations process (unavailability of end user does not impact metric)</p> <p><i>Rollbacks:</i> <Two (2) for Task Order</p> <p>>97% deployments require no Emergency Release</p>	<p>OCIO/CCHQ Install error log,</p> <p>OCIO/CCHQ Change Request</p> <p>OCIO/CCHQ CM Build Report</p>

3C	Post Deployment Reliability***	<p>This metric measures the reliability of software deployments.</p> <p>Reliability measures the failure-free**** operations during an interval of time.</p>	<p><i>Event/Problem/Issue Discovered in 24 hours:</i></p> <ul style="list-style-type: none"> • Severity Level 1: < Two (2) per Task Order • Severity Level 2: < Three (3) per Task Order • Severity Level 3: < Five (5) per Task Order • Severity Level 4: < Five (5) per Task Order <p><i>Event/Problem/Issue Discovered within One (1) week:</i></p> <ul style="list-style-type: none"> • Severity Level 1: < Two (2) per Task Order • Severity Level 2: < Five (5) per Task Order • Severity Level 3: < Seven (7) per Task Order • Severity Level 4: < Seven (7) per Task Order <p><i>Event/Problem/Issue Discovered within One (1) month:</i></p> <ul style="list-style-type: none"> • Severity Level 1: < Two (2) per Task Order • Severity Level 2: < Five (5) per Task Order • Severity Level 3: < Ten (10) per Task Order • Severity Level 4: < Ten 	<p>Service Desk</p> <p>Problem Alerts</p> <p>Problem Notifications</p> <p>CCHQ email</p>
----	--------------------------------------	--	---	--

Item #	Requirements	Description	Specifications	Measurement Vehicle
			(10) per Task Order	

*** Events/Problems/Issues determined (in the Root Cause Analysis report) to be due to factors other than the application or the actions of the Contractor are excluded from the metric calculations.

**** Failed/Failure Rate/Failure-free are each measured within the software release test plan. Every release has a test plan that has test cases. Every test case has a singular result identified as **Pass/Fail**.

Section 4: Administrative/Project Management

Table 2 Reference	Requirements	Description	Specifications	
4A	Project Management	The vendor will provide project management services and documentation to ensure full transparency of system performance, schedule, and cost objectives consistent with PMBOK and HHS EPLC.	<p>>95% within One (1) business day</p> <p>>99% within Two (2) business days</p>	OCIO/CCHQ email

Table 2 Reference	Requirements	Description	Specifications	
4B	Project Deliverables	This metric measures delivery milestones based on project schedule.	<p><i>Schedule variance: <10%</i></p> <p><i>Request for task/deliverable schedule relief/waivers: <5% of total number of tasks due to Contractor events</i></p>	<p>Project Plan</p> <p>Problem Notices generate by the Contractor</p>
4C	Project Schedule	This metric measures the timeliness of responses to information requests. The timeliness for the customer and technical support to contact the call/email originator, acknowledging receipt. Support staff and customer subject matter experts (SMEs) shall respond to correspondence and messages within acceptable guidance.	<p>Communications initiated by sender shall be responded to within forty-eight (48) hours from receipt</p> <p><i>***This metric does NOT supersede Section 2: Operations/Problems Management requirements</i></p>	<p>OCIO/CCHQ email/call</p> <p>Vendor email/call</p>
4D	Support Schedule	This metric measures the timeliness of responses for	Communications initiated by sender between the hours of 8:00 am to 2:00 pm shall be responded to within four	OCIO/CCHQ email

Table 2 Reference	Requirements	Description	Specifications	
		technical support. Staff shall respond to correspondence and voice, to acknowledge receipt, within acceptable guidance.	<p>(4) hours the same business day</p> <p>Communication initiated by sender between 2:00 pm and 8:00 am shall be answered NLT 10:00 am the next business day</p> <p><i>***This metric does NOT supersede Section 2: Operations/Problems Management requirements</i></p>	

**** Events/Problems/Issues determined (in the Root Cause Analysis report) to be due to factors other than the application or the actions of the Contractor are excluded from the metric calculations.*

Section 5: Problem Severity Definitions (Table(s) on pages 78-82)

Description	Definition
<p>Severity Level 1 Emergency/Urgent (Critical Business Impact)</p>	<p>The incident has affected a critical functional or critical infrastructure component, causing a complete and immediate work stoppage for a primary business process or a broad group of users. Examples include:</p> <ul style="list-style-type: none"> • Major application or database is disabled or unavailable to users (e.g., Online Pay Program or Leave Program is not available) • Severe disruption during critical periods (e.g., post-payroll processing) • Security violation (e.g., denial of service)
<p>Severity Level 2 High (Major Business Impact)</p>	<p>The incident has affected a business function to be severely degraded or a critical function to operate at a significantly reduced capacity or functionality impacting multiple users and key customers. Examples include:</p> <ul style="list-style-type: none"> • Substantial decrease in user-perceived end-to-end performance due to a database performance problem, network congestion, etc. • Support system outage (e.g., AMS, COPPS, etc.) • Interface outage (e.g., AMS, SOAP and eOPF interfaces) • Application outage (e.g., PO Close and Payroll Processing)
<p>Severity Level 3 Medium (Moderate Business Impact)</p>	<p>The incident has caused a business process to be affected in such a way that certain functions are unavailable to end users or a system and/or service is degraded. A workaround may be available. Examples include:</p> <ul style="list-style-type: none"> • Temporary unavailability of an infrequently used function within an application (e.g., specific bulk and individual NoA and wizard functions) • Localized network congestion results in slow performance for a small percentage of application functions

Severity Level 4 Low (Minimal Business Impact)	<p>The incident has little impact on normal business processes and can be handled on a scheduled basis. A workaround is available or there is minimal negative impact on a user's ability to perform their normal daily work. Examples include:</p> <ul style="list-style-type: none"> • “How To” questions • Service Request (e.g., system enhancement) • Peripheral problems (e.g., sign-on issues, browser issues) • Preventive maintenance
--	--

Section 6: Bug fix Review Definitions

Description	Definition
Rejected	<p>The bug fix review cannot feasibly be continued and is rejected by the reviewer. Examples include:</p> <ul style="list-style-type: none"> • The quality of the bug fix is too low to continue the bug fix review, e.g., too many errors in the fix. • The formatting of the bug fix does not follow OCIO/CCHQ coding standard such that the readability of the bug fix is so low to continue the bug fix review.
Severe	<p>The defect has to be fixed before going production. No exception will be granted. Examples include:</p> <ul style="list-style-type: none"> • Possibility of null pointer exception • Uninitiated read of field in constructor declaration • Incorrect overriding methods, such as the equals (), hashBug fix () and toString() from the Object class in Java • Race condition • Fail to validate untrusted input to the component • Use clear passwords • Risk of cross-site scripting, SQL injection, etc. • Use in-line queries • Input fields without parameterized validations.

Major	<p>The defect has to be fixed before going production unless an exception is granted. Examples include:</p> <ul style="list-style-type: none"> • Insufficient exception handling • Incorrect calling methods from the base classes • Un-closed resources, such as files, streams, memory, and db connections, etc. • Cause data contamination • Use incorrect encoding • Unnecessary network and database access • Insufficient network or database access, log in exception handling • Use over complicated technology stack when a simpler stack is possible. • Insufficient unit test. • Hard bug fixed variables that may change including environmental/configuration information
Minor	<p>The defect does not impact daily operations of the software. It will be fixed in current or future releases. Examples include:</p> <ul style="list-style-type: none"> • Insufficient comments • Nonconformance to OCIO/CCHQ naming or numbering standard • Too many lines of bug fix in a file or in a method • Lines too long • Inefficient use of Java (e.g., Collections framework, iteration mechanism)

ADDITIONAL HSPD-12 REQUIREMENTS

Important Note to Contractor: In the event of a discrepancy between the following language and included HHSAR clauses, the HHSAR clauses take precedence.

To perform the work specified herein, contractor personnel will require access to proprietary, privacy protected and/or sensitive data, regular access to HHS-controlled facilities and/or access to HHS information systems. In addition to requirements stated elsewhere in this contract, the contractor shall comply with the following.

Contractor personnel subject to HSPD-12 credentialing requirements may not begin work requiring access to HHS facilities, information or information systems until codified credentialing standards are met and the HSPD12 badges have been issued.

The minimum Government investigation to receive an HSPD-12 PIV Credential is a Tier 1 (NACI), which consists of searches of records covering specific areas of a person's background during the past five years. The minimum Government investigation to receive Elevated Privilege (any access beyond normal email or data entry) is a Tier 4 (BI High Risk Public Trust).

The contractor must comply with the instructions and timeframes provided by the Contracting Officer's Representative (COR) regarding the handling of the security requirements specified in this section. Typically, each employee must submit at a minimum: a completed OF-306; a current resume; and a completed HHS 828 form. Additional requirements may apply to Foreign National Applicants who will follow a slightly different level of initial checks. Contractors should ensure that the employees whose names they submit have a reasonable chance for access approval. In some cases, employees with existing background investigations commensurate with sensitivity designations will expedite performance. Inquiries, including requests for forms and assistance, should be directed to the COR.

Typically, the Government investigates personnel at no cost to the contractor, but the expense of multiple investigations for the same position is difficult to justify. Consequently, multiple investigations for the same position may, at the Contracting Officer's discretion, justify reduction(s) in the contract price of no more than the cost of the extra investigation(s).

After final acceptance of the work specified herein or any employee departure, the contractor shall follow the COR's instruction on the return of all identification badges, building access cards, Government Furnished Equipment, Government Furnished Data and Government Furnished Property (GFE/GFD/GFP) as applicable.

HHS reserves the right to suspend or withdraw access at any time for any reason.

Language similar to this Security section shall be included in any subcontracts which require access to proprietary, privacy protected and/or sensitive data, regular access to HHS-controlled facilities and/or access to HHS information systems.

SECTION D - Packaging and Marking

D.1 PACKAGING AND MARKING

All deliverables shall be delivered to the Contracting Officer's Representative (COR) identified in Section G and shall be marked as follows:

1. Name and address of the Contractor;
2. Contract Number;
3. Description of item contained therein; and
4. Consignee's name and address.

D.2 PAYMENT OF POSTAGE AND FEES

All postage and fees related to submitting information including forms, reports, etc. to the Contracting Officer or COR shall be paid by the Contractor.

SECTION E - Inspection and Acceptance

E.1 INSPECTION AND ACCEPTANCE

Pursuant to FAR clause 52.212-4, all work described in Section C to be delivered under this contract is subject to final inspection and acceptance by an authorized representative of the Government. The authorized representative of the Government is the Contracting Officer's Representative (COR), who is responsible for inspection and acceptance of all services, materials, or supplies to be provided by the Contractor.

E.1.1 Inspection and Acceptance Criteria

Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery by the COR.

E.1.2 General Acceptance Criteria

General quality measures, as set forth below, will be applied to each work product received from the Contractor under this Statement of Work.

- Accuracy - Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity - Work Products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
- Consistency to Requirements - All work products must satisfy the requirements of this Statement of Work.
- File Editing - All text and diagrammatic files shall be editable by the Government.
- Format - Work Products shall be submitted in hard copy and electronic copy. The electronic copy must be in a format as indicated in the Deliverables Table.

SECTION F - Deliveries or Performance

F.1 PERIOD OF PERFORMANCE – Severable Services

The base period of performance includes a 2-month Transition Period, a base period of 6-months, one 6-month option period. The contract is also incorporating four (4), one-year option periods as follows:

Base Period:

(2 months) CLIN 1001 Transition-In Optional Period*: November 1, 2024 – December 31, 2024

(6 months) CLIN 1002 and CLIN 1004 - January 1, 2025 to July 1, 2025

(6 months) CLIN 1003 and CLIN 1005 - July 2, 2025 to December 31, 2025

*The Government anticipates exercising the Transition-In Optional Period unless the recipient of the subject recompete award is the incumbent, in which the performance periods will be adjusted.

Option Period 1: CLIN 2002 and CLIN 2003 - January 1, 2026 – December 31, 2026

Option Period 2: CLIN 3002 and CLIN 3003 - January 1, 2027 – December 31, 2027

Option Period 3: CLIN 4002 and CLIN 4003 - January 1, 2028 – December 31, 2028

Option Period 4: CLIN 5002 and CLIN 5003 - January 1, 2029 – October 31, 2029

Option periods may be exercised in accordance with FAR Clause 52.217-9 entitled "Option to Extend the Term of the Contract."

F.2 PLACE OF PERFORMANCE

Work will be performed at: 1201 Seven Locks Road, Suite 360-22 Rockville, MD. 20854, except for work permitted to be performed via alternate site, such as via telework, if specifically allowed elsewhere in the contract. The Contracting Officer's Representative has the authority to approve and reject requests to work at alternate sites, and rescind requests previously approved. See F.4 of the contract regarding Government site closures.

F.3 DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall submit all required report(s)/deliverables in accordance with the following schedule: All reports shall reference and cite the contract number.

The following table details a listing of possible Contractor deliverables for each section that may be included in the Schedule of Deliverables in procurement documentation. Please note that this list only includes the minimum deliverables and additional contract deliverables may apply. Consult with your security and privacy officials to determine the complete list.

Deliverable	Section/Deliverable Description	Due Date
-------------	---------------------------------	----------

Transition In Plan	Detail Plan outlining methods for smooth transition from incumbent Contractor to successor Contractor	5 Business Days from Contract Award Date
Transition In Period and Services	Execute Transition In Plan and Provide Transition-In Services	Not to exceed 60 days post Contract Award Date, Must be completed by 1/1/25.
Transition Out Plan	Develop a transition-out plan for transferring service responsibility from this award to another provider or back to CCHQ	90 business days prior to contract expiration
Transition Out Period and Services	Execute Transition Out Plan and Provide Transition-Out Services	Not to exceed 60 days
Collaboration Plan w/Outgoing Contractor	Plan for collaborative efforts with the outgoing contractor to ensure seamless transition activities	5 Business Days from Contract Award Date
Fulfillment of Key Positions	Ensure all key positions for all labor categories are filled	Within 60 days of contract award
Obtain and Maintain ATO for SFTP Servicer	Obtain and maintain Authority to Operate (ATO) for Secure File Transfer Protocols (SFTP) data server.	30 Business Days before Service transition from incumbent to successor
Connectivity to Treasury	Obtain required connectivity to Treasury Department systems	Within 60 days of contract award
O&M Support Plan	Detailed plan outlining ongoing operations and maintenance support services to ensure system functionality	30 Business Days before Service transition from incumbent to successor
Helpdesk Support for Users	Procedures for providing helpdesk support to users for technical issues	30 Business Days before Service transition from incumbent to successor
Security Monitoring and Compliance	Procedures for monitoring system security and ensuring compliance with regulations	30 Business Days before Service transition from incumbent to successor
Disaster Recovery Planning and Execution	Plan for disaster recovery to ensure system availability in case of emergency	30 Business Days post contract award
Project Management Plan	Detailed plan defining organizational resources, processes and procedures associated with contract program management tasks and duties	Within 30 business days of contract award
Program Roadmap/Schedule	Schedule outline key activities and milestones for ongoing support services	Within 30 business days of contract award
Training and Knowledge Transfer Plan	Identification of training needs and transfer knowledge for staff involved in transition	Within 30 business days of contract award
User Manuals/ How-To Guides	Create user manuals and/or How-To guides to document the processes and functions for the new provider's personnel and payroll solution	1 st delivery 30 days post contract award 2 nd delivery 30 days prior to Go-Live/End of Transition-In Period

		3 rd as needed based on updates
Risk Management Process	Process for identifying and mitigating program risks, in compliance with EPLC standards	Within 2 weeks of kick-off
System Testing	Success completion of payroll and personal solution test	No later than December 16, 2024

Deliverable	Section/Deliverable Description	Due Date
Roster	Roster	Within 5 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 after 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	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	Incident and Breach Response Plan	60 days after work begins on contract.

Deliverable	Section/Deliverable Description	Due Date
Personnel Security Responsibilities	List of Personnel with defined roles and responsibilities	Within 5 days that is before an employee begins working on this contract.
Personnel Security Responsibilities	Off-boarding documentation, equipment and badge when leaving contract	Within 2 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	Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS
Certification of Sanitization of Government and Government Activity-Related Files, Information, and Devices. [28]	Form or deliverables required by OpDiv.	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.
Assessment and Authorization (A&A)	A&A Package <ul style="list-style-type: none"> • SSP • SAR • POA&M • Authorization Letter • CP and CPT Report • E-Auth (if applicable) • PTA/PIA (if applicable) 	<i>Deliverable timelines will be determined by the HHS and FedRAMP A&A guidance</i>

Deliverable	Section/Deliverable Description	Due Date
	<ul style="list-style-type: none"> • Interconnection/Data Use Agreements (if applicable) • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other OpDiv-specific documents 	
Protection of Information in a Cloud Environment	Contract expiration	Due in accordance with FedRAMP deliverable timeline guidance
A&A Process for Cloud Services	<p>A&A Package</p> <ul style="list-style-type: none"> • SSP • SAR • POA&M • CMP • CP and CPT Report • E-Auth (if applicable) • PTA/PIA (if applicable) • Penetration Test Results • Interconnection/Data Use/Agreements (if applicable) • Service Level Agreement • Authorization Letter • Configuration Management Plan (if applicable) • Configuration Baseline • Other OpDiv-specific documents 	Due in accordance with FedRAMP deliverable timelines guidance 30 days after contract award.
Reporting and Continuous Monitoring	POA&M updates Revised security documentation/Agreements	Monthly/as requested by OS/OASH CISO
Security Alerts, Advisories, and Directives	List of personnel with designated roles and responsibilities	30 days after contract award
Incident Reporting	Incident reports (as needed)	According to

Deliverable	Section/Deliverable Description	Due Date
	Incident Response Plan	HHS/OS Incident Response Guidance
Other IT Procurements (Non-Commercial and Open-Source Computer Software Procurements)	Computer software, including the source code.	Prior to performing any work on behalf of HHS

F.4 DELIVERY REQUIREMENTS

Pickup and delivery of items under this contract shall be accomplished between the hours of [8:30 a.m. and 4:00 p.m.], Monday through Friday unless changed by mutual agreement between the COR and the contractor. No deliveries shall be made on Saturdays, Sundays, and days of government closure or Federal legal holidays found at:
http://www.opm.gov/operating_status_schedules.

F.5 OBSERVANCE OF LEGAL HOLIDAYS AND DAYS OF GOVERNMENT CLOSURE – ONSITE CONTRACTOR EMPLOYEES

- (a)(1) The performance of this contract requires contractor employees of the prime contractor or any subcontractor, affiliate, partner, joint venture, or team member with which the contractor is associated, including consultants engaged by any of these entities, to have access to, physical entry into, and to the extent authorized, mobility within, a Federal facility.
 - (2) The Government may close and or deny contractor access to a Federal facility for a portion of a business day or longer due to any one of the following events:
 - (i) Federal public holidays for federal employees in accordance with 5 U.S.C. 6103.
 - (ii) Fires, floods, earthquakes, unusually severe weather to include snow storms, tornadoes and hurricanes.
 - (iii) Occupational safety or health hazards.
 - (iv) Any other reason.
 - (3) In such events, the contractor employees may be denied access to a Federal facility, in part or in whole, to perform work required by the contract. Contractor personnel already present at a Federal facility during such events may be required to leave the facility.
- (b) In all instances where contractor employees are denied access or required to vacate a Federal facility, in part or in whole, the contractor shall be responsible to ensure contractor personnel working under the contract comply. If the circumstances permit, the contracting officer or contracting officer's representative will provide direction to the contractor, which could include continuing on-site performance during the Federal facility closure period. In the absence of such direction, the contractor shall exercise sound judgment to minimize unnecessary contract costs

and performance impacts by, for example, performing required work off-site if possible or reassigning personnel to other activities if appropriate.

(c) The contractor shall be responsible for monitoring when the Federal facility becomes accessible and shall resume contract performance as required by the contract.

(d) For the period that Federal facilities were not accessible to contractor employees, the contracting officer may—

(1) Adjust the contract performance or delivery schedule for a period equivalent to the period the Federal facility was not accessible;

(2) Forego the work;

(3) Reschedule the work by mutual agreement of the parties; or

(4) Consider properly documented requests for equitable adjustment, claim, or any other remedy pursuant to the terms and conditions of the contract.

SECTION G - Contract Administration Data

G.1 CONFERENCE EXPENSES

Unless the Contracting Officer provides explicit written approval for conference expenses, conference expenses are not allowable under this contract. For purposes of this contract, conference and conference expense are defined in the HHS Policy on Promoting Efficient Spending, specifically Attachment 1, Use of Appropriated Funds for Conferences and Meeting Space dated January 23, 2015. The attachment also provides a list of typical HHS meetings and events that are not considered conferences at Exhibit 2. The policy and associated attachments are located at the following site:

<http://www.hhs.gov/grants/contracts/contract-policies-regulations/index.html>)

G.2 AUTHORITIES OF GOVERNMENT PERSONNEL

Notwithstanding the Contractor's responsibility for total management during the performance of this contract, the administration of this contract will require maximum coordination between the Government and the Contractor. The following individuals will be the Government's points of contact during the performance of this contract:

Contracting Officer

Name: Anne Mineweaser

Phone: (301)-492-4606

Email: anne.mineweaser@psc.hhs.gov

All communications pertaining to contractual and/or administrative matters under this contract shall be sent to:

Contract Specialist

Name: Jacob Matthews

Phone: 385-285-7382

Email: Jacob.matthews@psc.hhs.gov

Contracting Officer's Representative

Name: TBD

Phone: TBD

Email: TBD

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

G.6 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AUTHORITY

(a) Performance of work under this contract must be subject to the technical direction of the

Contracting Officer's Representative identified above, or a representative designated in writing. The term "technical direction" includes, without limitation, direction to the contractor that directs or redirects the labor effort, shifts the work between work areas or locations, fills in details and otherwise serves to ensure that tasks outlined in the work statement are accomplished satisfactorily.

(b) Technical direction must be within the scope of the specification(s)/work statement.

The Contracting Officer's Representative does not have authority to issue technical direction that:

(1) Constitutes a change of assignment or additional work outside the specification(s)/statement of work;

(2) Constitutes a change as defined in the clause entitled "Changes";

(3) In any manner causes an increase or decrease in the contract price, or the time required for contract performance;

(4) Changes any of the terms, conditions, or specification(s)/work statement of the contract;

(5) Interferes with the contractor's right to perform under the terms and conditions of the contract; or

(6) Directs, supervises or otherwise controls the actions of the contractor's employees.

(c) Technical direction may be oral or in writing. The Contracting Officer's Representative shall confirm oral direction in writing within five work days, with a copy to the Contracting Officer.

(d) The contractor shall proceed promptly with performance resulting from the technical direction issued by the Contracting Officers, Representative. If, in the opinion of the contractor, any direction of the Contracting Officers, Representative, or his/her designee, falls within the limitations in (b), above, the contractor shall immediately notify the Contracting Officer no later than the beginning of the next Government work day.

(e) Failure of the contractor and the Contracting Officer to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled "Disputes."



GOVERNMENT-FURNISHED PROPERTY

The Government will provide the following items(s) of Government property to the Contractor for use in the performance of this contract. The property shall be used and maintained by the Contractor in accordance with the HHS Contractors' Guide for Control of Government Property (Appendix Q of the HHS Logistics Management Manual) found at

<https://web.archive.org/web/20111015044731/http://www.hhs.gov/hhsmanuals/>. The Contractor shall be responsible and accountable for all government property; either furnished or acquired, and also is required to keep the Government's official records of Government property in their possession and control. The following item(s) of Government property are hereby furnished to the Contractor:

Item	Description	Quantity	Government Serial Number
------	-------------	----------	--------------------------

Government will provide laptops.

G.8 CONTRACTOR-ACQUIRED PROPERTY -- Reserved

The Contractor is hereby authorized to purchase the following equipment for use in the performance under this contract. It is understood and agreed to that title to the following equipment shall vest in the Government. The authorized equipment is as follows:

Item	Description	Quantity	Cost
[***insert table]			

G.9 INVOICES

Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP)

- All Invoice submissions for goods and or services delivered to facilitate payments must be made electronically through the U.S. Department of Treasury's Invoice Processing Platform System (IPP).
- Invoice Submission for Payment means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 included in commercial items contracts. The IPP website address is: <https://www.ipp.gov>.
- The Agency will enroll the Contractors new to IPP. The Contractor must follow the IPP registration email instructions for enrollment to register the Collector Account for submitting invoice requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive Registration email from the Federal Reserve Bank of St. Louis (FRBSTL) within 3 – 5 business days of the contract award for new contracts or date of modification for existing contracts.
 - Registration emails are sent via email from ipp.noreply@mail.ero.c.twai.gov. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email to IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973-3131.
 - The Contractor POC will receive two emails from **IPP Customer Support**, the first email contains the initial administrative IPP User ID. The second email, sent within 24 hours of receipt of the first email, contains a temporary password. You must log in with the temporary password within 30 days.
- If your company is already registered to use IPP, you will not be required to re-register.

- If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment as authorized by HHSAR 332.7002, a written request must be submitted to the Contracting Officer to explain the circumstances that require the authorization of alternate payment procedures.

Additional Office of Acquisition Management Services (OAMS) requirements:

- (i) The contractor shall submit invoices under this contract once per month. For indefinite delivery vehicles, separate invoices must be submitted for each order.
- (ii) Invoices must break-out price/cost by contract line item number (CLIN) as specified in the pricing section of the contract.
- (iii) Invoices that include time and materials or labor hours CLINS must include supporting documentation to (1) substantiate the number of labor hours invoiced for each labor category, and (2) substantiate material costs incurred (when applicable).
- (iv) Invoices submitted to IPP are limited to 10MB. Backup support should be sent to the contracting officer, contract specialist, and COR in the event it causes the file size to exceed the limit.

SECTION H - Special Contract Requirements

H.1 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): <http://www.acquisition.gov/far/>

H.2 KEY PERSONNEL

In accordance with the key personnel terms included in the contract, key personnel are as follows:

<u>Name</u>	<u>Position Title</u>
-------------	-----------------------

H.3 PROHIBITION AGAINST PERSONAL SERVICES

The Contractor shall not perform personal services under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently-governmental functions under this contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

H.4 CONTRACTOR PERFORMANCE EVALUATION(S) –

Contractor performance will be evaluated on an interim and final basis pursuant to FAR Subpart 42.15. Interim evaluations will occur on an annual basis upon the completion of the first year of the contract. The Contractor Performance Assessment Reporting System (CPARS) will be used for these reviews. Information on CPARS is located at <http://www.cpars.gov>.

Contractors may, at their discretion, request to submit a self-assessment to the COR and

contracting officer to consider when documenting performance, at no additional cost. The self-assessment should be submitted to the COR and contracting officer at least 30 days prior to completion of the first year, and each following year. Please request the self-assessment from the contracting officer. The Self-assessment should be submitted to the COR and contracting Officer at least 30 days prior to the execution of any option year/period, and the completion of the base period of performance.

H.5 POST AWARD ORGANIZATIONAL CONFLICT OF INTEREST

a. General: The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.

b. Disclosure: The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contract or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.

c. Resolution: In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include, but is not limited to, requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.

H.6 DEPARTMENT OF LABOR WAGE DETERMINATIONS

The below Department of Labor Wage Determinations are hereby incorporated into the contract:

Not Applicable.

H.7 EQUAL EMPLOYMENT OPPORTUNITY POSTERS

In order to comply with the notice posting requirements of FAR clause 52.222-26 Equal Opportunity as incorporated into the contract, the contractor shall obtain the posters from the following link: <https://www1.eeoc.gov/employers/poster.cfm>.

H.8 CONTRACTOR PERSONNEL IDENTIFICATION

Contractor and subcontractor employees are required to identify themselves as contractor personnel in all contract related meetings with government personnel, or the general public, and in all contract related communication, to include oral and written correspondence.

At a minimum, emails and voicemails shall include the following details:

Name, Functional Job Title

Contractor Company Name

On assignment with:

Applicable HHS Office

Other contact details as necessary

H.9 SAFEGUARDING FEDERAL TAX INFORMATION

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor.
- (2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the

requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

(8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

(9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

(10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in

an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

SECTION I - Contract Clauses

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) AND HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) CONTRACT CLAUSES

I.1 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):

<http://www.acquisition.gov/far/> and <https://www.acquisition.gov/hhsar>

FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) CLAUSES

FAR 52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)
FAR 52.204-16	Commercial and Government Entity Code Reporting (Aug 2020)
FAR 52.204-17	Ownership or Control of Offeror (Aug 2020)
FAR 52.204-18	Commercial and Government Entity Code Maintenance (Aug 2020)
FAR 52.204-22	Alternative Line Item Proposal (Jan 2017)
FAR 52.232-23	Assignment of Claims (May 2017)
FAR 52.233-1	Disputes (May 2014)
FAR 52.246-4	Inspection of Services-Fixed-Price (Aug 1996)
FAR 52.249-4	Termination for Convenience of the Government (Services) (Short Form) (Apr 1984)
FAR 52.212-4	Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023)
FAR 52.232-39	Unenforceability of Unauthorized Obligations (Jun 2013)

HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) CLAUSES

352.203-70	Anti-lobbying (DEC 2015)
352.208-70	Printing and Duplication (DEC 2015)
352.211-3	Paperwork Reduction Act (DEC 2015)
352.222-70	Contractor Cooperation in Equal Employment Opportunity Investigations. (DEC 2015)
352.232-71	Electronic Submission of Payment Requests (FEB 2022)
352.237-75	Key Personnel (DEC 2015)
352.239-73	Electronic and Information Technology Accessibility Notice (DEC 2015)
352.270-74	Electronic and Information Technology Accessibility (DEC 2015)

I.2 FAR CLAUSES IN FULL TEXT

I.2.1 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT

STATUTES OR EXECUTIVE ORDERS-COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (MAY 2024)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

(1) [52.203-19](#), Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) [52.204-23](#), Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (DEC 2023) (Section 1634 of Pub. L. 115-91).

(3) [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) [52.209-10](#), Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) [52.232-40](#), Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) ([31 U.S.C. 3903](#) and [10 U.S.C. 3801](#)).

(6) [52.233-3](#), Protest After Award (AUG 1996) ([31 U.S.C. 3553](#)).

(7) [52.233-4](#), Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77 and 108-78 ([19 U.S.C. 3805 note](#))).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[Contracting Officer check as appropriate.]

 X (1) [52.203-6](#), Restrictions on Subcontractor Sales to the Government (JUN 2020), with *Alternate I* (Nov 2021) ([41 U.S.C. 4704](#) and [10 U.S.C. 4655](#)).

 X (2) [52.203-13](#), Contractor Code of Business Ethics and Conduct (Nov 2021) ([41 U.S.C. 3509](#))).

__ (3) [52.203-15](#), Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

X (4) [52.203-17](#), Contractor Employee Whistleblower Rights (Nov 2023) ([41 U.S.C. 4712](#)); this clause does not apply to contracts of DoD, NASA, the Coast Guard, or applicable elements of the intelligence community—see FAR [3.900](#)(a).

X (5) [52.204-10](#), Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020) (Pub. L. 109-282) ([31 U.S.C. 6101 note](#)).

__ (6) [Reserved].

X (7) [52.204-14](#), Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

__ (8) [52.204-15](#), Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

X (9) [52.204-27](#), Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

__ (10) [52.204-28](#), Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (DEC 2023) ([Pub. L. 115-390](#), title II).

__ (11) (i) [52.204-30](#), Federal Acquisition Supply Chain Security Act Orders—Prohibition. (DEC 2023) ([Pub. L. 115-390](#), title II).

__ (ii) Alternate I (DEC 2023) of [52.204-30](#).

X (12) [52.209-6](#), Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Nov 2021) ([31 U.S.C. 6101 note](#)).

X (13) [52.209-9](#), Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018) ([41 U.S.C. 2313](#)).

__ (14) [Reserved].

__ (15) [52.219-3](#), Notice of HUBZone Set-Aside or Sole-Source Award (OCT 2022) ([15 U.S.C. 657a](#)).

__ (16) [52.219-4](#), Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2022) (if the offeror elects to waive the preference, it shall so indicate in its offer) ([15 U.S.C. 657a](#)).

__ (17) [Reserved]

X (18) (i) [52.219-6](#), Notice of Total Small Business Set-Aside (Nov 2020) ([15 U.S.C. 644](#)).

__ (ii) Alternate I (MAR 2020) of [52.219-6](#).

__ (19) (i) [52.219-7](#), Notice of Partial Small Business Set-Aside (Nov 2020) ([15 U.S.C. 644](#)).

__ (ii) Alternate I (MAR 2020) of [52.219-7](#).

X (20) [52.219-8](#), Utilization of Small Business Concerns (FEB 2024)
([15 U.S.C. 637\(d\)\(2\)](#) and (3)).

__ (21) (i) [52.219-9](#), Small Business Subcontracting Plan (SEP 2023) ([15 U.S.C. 637\(d\)\(4\)](#)).

__ (ii) Alternate I (Nov 2016) of [52.219-9](#).

__ (iii) Alternate II (Nov 2016) of [52.219-9](#).

__ (iv) Alternate III (JUN 2020) of [52.219-9](#).

__ (v) Alternate IV (SEP 2023) of [52.219-9](#).

__ (22) (i) [52.219-13](#), Notice of Set-Aside of Orders (MAR 2020) ([15 U.S.C. 644\(r\)](#)).

__ (ii) Alternate I (MAR 2020) of [52.219-13](#).

X (23) [52.219-14](#), Limitations on Subcontracting (OCT 2022) ([15 U.S.C. 637s](#)).

X (24) [52.219-16](#), Liquidated Damages—Subcontracting Plan (SEP 2021) ([15 U.S.C. 637\(d\)\(4\)\(F\)\(i\)](#)).

__ (25) [52.219-27](#), Notice of Set-Aside for, or Sole-Source Award to, Service-Disabled Veteran-Owned Small Business (SDVOSB) Concerns Eligible Under the SDVOSB Program (FEB 2024) ([15 U.S.C. 657f](#)).

X (26) (i) [52.219-28](#), Post Award Small Business Program Rerepresentation (FEB 2024) ([15 U.S.C. 632\(a\)\(2\)](#)).

__ (ii) Alternate I (MAR 2020) of [52.219-28](#).

__ (27) [52.219-29](#), Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (OCT 2022) ([15 U.S.C. 637\(m\)](#)).

__ (28) [52.219-30](#), Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (OCT 2022) ([15 U.S.C. 637\(m\)](#)).

__ (29) [52.219-32](#), Orders Issued Directly Under Small Business Reserves (MAR 2020) ([15 U.S.C. 644\(r\)](#)).

__ (30) [52.219-33](#), Nonmanufacturer Rule (SEP 2021) ([15U.S.C. 637\(a\)\(17\)](#)).

X (31) [52.222-3](#), Convict Labor (JUN 2003) (E.O.11755).

__ (32) [52.222-19](#), Child Labor-Cooperation with Authorities and Remedies (FEB 2024).

X (33) [52.222-21](#), Prohibition of Segregated Facilities (APR 2015).

X (34) (i) [52.222-26](#), Equal Opportunity (SEP 2016) (E.O.11246).

__ (ii) Alternate I (FEB 1999) of [52.222-26](#).

X (35) (i) [52.222-35](#), Equal Opportunity for Veterans (JUN 2020) ([38 U.S.C. 4212](#)).

__ (ii) Alternate I (JUL 2014) of [52.222-35](#).

X (36) (i) [52.222-36](#), Equal Opportunity for Workers with Disabilities (JUN 2020) ([29 U.S.C. 793](#)).

__ (ii) Alternate I (JUL 2014) of [52.222-36](#).

X (37) [52.222-37](#), Employment Reports on Veterans (JUN 2020) ([38 U.S.C. 4212](#)).

X (38) [52.222-40](#), Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

X (39) (i) [52.222-50](#), Combating Trafficking in Persons (Nov 2021) ([22 U.S.C. chapter 78](#) and E.O. 13627).

__ (ii) Alternate I (MAR 2015) of [52.222-50](#) ([22 U.S.C. chapter 78](#) and E.O. 13627).

X (40) [52.222-54](#), Employment Eligibility Verification (MAY 2022) (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR [22.1803](#).)

__ (41) (i) [52.223-9](#), Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) ([42 U.S.C. 6962\(c\)\(3\)\(A\)\(ii\)](#)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

— (ii) Alternate I (MAY 2008) of [52.223-9](#) ([42 U.S.C. 6962\(i\)\(2\)\(C\)](#)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

— (42) [52.223-11](#), Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (MAY 2024) ([42 U.S.C. 7671](#), *et seq.*).

— (43) [52.223-12](#), Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (MAY 2024) ([42 U.S.C. 7671](#), *et seq.*).

— (44) [52.223-20](#), Aerosols (MAY 2024) ([42 U.S.C. 7671](#), *et seq.*).

— (45) [52.223-21](#), Foams (MAY 2024) ([42 U.S.C. 7671](#), *et seq.*).

X (46) [52.223-23](#), Sustainable Products and Services (MAY 2024) ([E.O. 14057](#), [7 U.S.C. 8102](#), [42 U.S.C. 6962](#), [42 U.S.C. 8259b](#), and [42 U.S.C. 7671i](#)).

X (47)(i) [52.224-3](#) Privacy Training (JAN 2017) (5 U.S.C. 552 a).

— (ii) Alternate I (JAN 2017) of [52.224-3](#).

— (48)(i) [52.225-1](#), Buy American-Supplies (OCT 2022) ([41 U.S.C. chapter 83](#)).

— (ii) Alternate I (OCT 2022) of [52.225-1](#).

— (49) (i) [52.225-3](#), Buy American-Free Trade Agreements-Israeli Trade Act (NOV 2023) ([19 U.S.C. 3301 note](#), [19 U.S.C. 2112 note](#), [19 U.S.C. 3805 note](#), [19 U.S.C. 4001 note](#), [19 U.S.C. chapter 29](#) (sections 4501-4732), [Public Law 103-182](#), [108-77](#), [108-78](#), [108-286](#), [108-302](#), [109-53](#), [109-169](#), [109-283](#), [110-138](#), [112-41](#), [112-42](#), and [112-43](#)).

— (ii) Alternate I [Reserved].

— (iii) Alternate II (DEC 2022) of [52.225-3](#).

— (iv) Alternate III (FEB 2024) of [52.225-3](#).

— (v) Alternate IV (Oct 2022) of [52.225-3](#).

— (50) [52.225-5](#), Trade Agreements (NOV 2023) ([19 U.S.C. 2501](#), *et seq.*, [19 U.S.C. 3301 note](#)).

— (51) [52.225-13](#), Restrictions on Certain Foreign Purchases (FEB 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

__ (52) [52.225-26](#), Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

__ (53) [52.226-4](#), Notice of Disaster or Emergency Area Set-Aside (Nov 2007) ([42 U.S.C. 5150](#)).

__ (54) [52.226-5](#), Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) ([42 U.S.C. 5150](#)).

X (55) [52.226-8](#), Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024) ([E.O. 13513](#)).

__ (56) [52.229-12](#), Tax on Certain Foreign Procurements (FEB 2021).

__ (57) [52.232-29](#), Terms for Financing of Purchases of Commercial Products and Commercial Services (Nov 2021) ([41 U.S.C. 4505](#), [10 U.S.C. 3805](#)).

__ (58) [52.232-30](#), Installment Payments for Commercial Products and Commercial Services (Nov 2021) ([41 U.S.C. 4505](#), [10 U.S.C. 3805](#)).

X (59) [52.232-33](#), Payment by Electronic Funds Transfer-System for Award Management (OCT2018) ([31 U.S.C. 3332](#)).

__ (60) [52.232-34](#), Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) ([31 U.S.C. 3332](#)).

__ (61) [52.232-36](#), Payment by Third Party (MAY 2014) ([31 U.S.C. 3332](#)).

X (62) [52.239-1](#), Privacy or Security Safeguards (AUG 1996) ([5 U.S.C. 552a](#)).

X (63) [52.242-5](#), Payments to Small Business Subcontractors (JAN 2017) ([15 U.S.C. 637\(d\)\(13\)](#)).

__ (64) (i) [52.247-64](#), Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) ([46 U.S.C. 55305](#) and [10 U.S.C. 2631](#)).

__ (ii) Alternate I (APR 2003) of [52.247-64](#).

__ (iii) Alternate II (Nov 2021) of [52.247-64](#).

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[Contracting Officer check as appropriate.]

__ (1) [52.222-41](#), Service Contract Labor Standards (AUG 2018) ([41 U.S.C. chapter 67](#)).

__ (2) [52.222-42](#), Statement of Equivalent Rates for Federal Hires (MAY 2014) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#)).

__ (3) [52.222-43](#), Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (AUG 2018) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#)).

__ (4) [52.222-44](#), Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (May 2014) ([29 U.S.C. 206](#) and [41 U.S.C. chapter 67](#)).

__ (5) [52.222-51](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) ([41 U.S.C. chapter 67](#)).

X (6) [52.222-53](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) ([41 U.S.C. chapter 67](#)).

X (7) [52.222-55](#), Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022).

X (8) [52.222-62](#), Paid Sick Leave Under Executive Order 13706 (JAN 2022) (E.O. 13706).

__ (9) [52.226-6](#), Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) ([42 U.S.C. 1792](#)).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR [2.101](#), on the date of award of this contract, and does not contain the clause at [52.215-2](#), Audit and Records-Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart [4.7](#), Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising

under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1), in a subcontract for commercial products or commercial services. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(i) [52.203-13](#), Contractor Code of Business Ethics and Conduct (Nov 2021) ([41 U.S.C. 3509](#)).

(ii) [52.203-17](#), Contractor Employee Whistleblower Rights (Nov 2023) ([41 U.S.C. 4712](#)).

(iii) [52.203-19](#), Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iv) [52.204-23](#), Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (DEC 2023) (Section 1634 of Pub. L. 115-91).

(v) [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(vi) [52.204-27](#), Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

(vii)

(A) 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (DEC 2023) ([Pub. L. 115-390](#), title II).

(B) Alternate I (DEC 2023) of 52.204-30.

(viii) [52.219-8](#), Utilization of Small Business Concerns (FEB 2024) ([15 U.S.C. 637\(d\)\(2\)](#) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold

specified in FAR [19.702\(a\)](#) on the date of subcontract award, the subcontractor must include [52.219-8](#) in lower tier subcontracts that offer subcontracting opportunities.

(ix) [52.222-21](#), Prohibition of Segregated Facilities (APR 2015).

(x) [52.222-26](#), Equal Opportunity (SEP 2015) (E.O.11246).

(xi) [52.222-35](#), Equal Opportunity for Veterans (JUN 2020) ([38 U.S.C. 4212](#)).

(xii) [52.222-36](#), Equal Opportunity for Workers with Disabilities (JUN 2020) ([29 U.S.C. 793](#)).

(xiii) [52.222-37](#), Employment Reports on Veterans (JUN 2020) ([38 U.S.C. 4212](#)).

(xiv) [52.222-40](#), Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause [52.222-40](#).

(xv) [52.222-41](#), Service Contract Labor Standards (AUG 2018) ([41 U.S.C. chapter 67](#)).

(xvi)

(A) [52.222-50](#), Combating Trafficking in Persons (Nov 2021) ([22 U.S.C. chapter 78](#) and E.O 13627).

(B) Alternate I (MAR 2015) of [52.222-50](#) ([22 U.S.C. chapter 78](#) and [E.O. 13627](#)).

(xvii) [52.222-51](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) ([41 U.S.C. chapter 67](#)).

(xviii) [52.222-53](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) ([41 U.S.C. chapter 67](#)).

(xix) [52.222-54](#), Employment Eligibility Verification (MAY 2022) (E.O. 12989).

(xx) [52.222-55](#), Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022).

(xxi) [52.222-62](#), Paid Sick Leave Under Executive Order 13706 (JAN 2022) (E.O. 13706).

(xxii)

(A) [52.224-3](#), Privacy Training (Jan 2017) ([5 U.S.C. 552a](#)).

(B) Alternate I (JAN 2017) of [52.224-3](#).

(xxiii) [52.225-26](#), Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

(xxiv) [52.226-6](#), Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) ([42 U.S.C. 1792](#)). Flow down required in accordance with paragraph (e) of FAR clause [52.226-6](#).

(xxv) [52.232-40](#), Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) ([31 U.S.C. 3903](#) and [10 U.S.C. 3801](#)). Flow down required in accordance with paragraph (c) of [52.232-40](#).

(xxvi) [52.247-64](#), Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) ([46 U.S.C. 55305](#) and [10 U.S.C. 2631](#)). Flow down required in accordance with paragraph (d) of FAR clause [52.247-64](#).

(2) While not required, the Contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

Alternate I (FEB 2000). As prescribed in [12.301](#) (b)(4)(i), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".

Alternate II (FEB 2024) . As prescribed in [12.301](#) (b)(4)(ii), substitute the following paragraphs (d)(1) and (e)(1) for paragraphs (d)(1) and (e)(1) of the basic clause as follows:

(d)(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8 G of the Inspector General Act of 1978 ([5 U.S.C. App.](#)), or an authorized representative of either of the foregoing officials shall have access to and right to—

(i) Examine any of the Contractor's or any subcontractors' records that pertain to, and involve transactions relating to, this contract; and

(ii) Interview any officer or employee regarding such transactions.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), and (c), of this clause, the Contractor is not required to flow down any FAR clause in a subcontract for commercial products or commercial services, other than—

(i) *Paragraph (d) of this clause.* This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (d)(1)(ii) does not flow down; and

(ii) *Those clauses listed in this paragraph (e)(1).* Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(A) [52.203-13](#), Contractor Code of Business Ethics and Conduct (Nov 2021) ([41 U.S.C. 3509](#)).

(B) [52.203-15](#), Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5).

(C) [52.203-17](#), Contractor Employee Whistleblower Rights (Nov 2023) ([41 U.S.C. 4712](#)).

(D) [52.204-23](#), Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (DEC 2023) (Section 1634 of Pub. L. 115-91).

(E) [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(F) [52.204-27](#), Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

(G) (1) [52.204-30](#), Federal Acquisition Supply Chain Security Act Orders—Prohibition. (DEC 2023) ([Pub. L. 115-390](#), title II).

—(2) Alternate I (DEC 2023) [52.204-30](#).

(H) [52.219-8](#), Utilization of Small Business Concerns (FEB 2024) ([15 U.S.C. 637\(d\)\(2\) and \(3\)](#)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR [19.702\(a\)](#) on the date of subcontract award, the subcontractor must include [52.219-8](#) in lower tier subcontracts that offer subcontracting opportunities.

(I) [52.222-21](#), Prohibition of Segregated Facilities (APR 2015).

(J) [52.222-26](#), Equal Opportunity (SEP 2016) (E.O. 11246).

(K) [52.222-35](#), Equal Opportunity for Veterans (JUN 2020) ([38 U.S.C. 4212](#)).

(L) [52.222-36](#), Equal Opportunity for Workers with Disabilities (JUN 2020) ([29 U.S.C. 793](#)).

(M) [52.222-40](#), Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause [52.222-40](#).

(N) [52.222-41](#), Service Contract Labor Standards (AUG 2018) ([41 U.S.C. chapter 67](#)).

(O) _ (1) [52.222-50](#), Combating Trafficking in Persons (Nov 2021) ([22 U.S.C. chapter 78](#) and E.O 13627).

_ (2) Alternate I (MAR 2015) of [52.222-50](#) ([22 U.S.C. chapter 78 and E.O. 13627](#)).

(P) [52.222-51](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) ([41 U.S.C. chapter 67](#)).

(Q) [52.222-53](#), Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) ([41 U.S.C. chapter 67](#)).

(R) [52.222-54](#), Employment Eligibility Verification (MAY 2022) (Executive Order 12989).

(S) [52.222-55](#), Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022).

(T) [52.222-62](#), Paid Sick Leave Under Executive Order 13706 (JAN 2022) (E.O. 13706).

(U)_ (1) [52.224-3](#), Privacy Training (JAN 2017) ([5 U.S.C. 552a](#)).

_ (2) Alternate I (JAN 2017) of [52.224-3](#).

(V) [52.225-26](#), Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

(W) [52.226-6](#), Promoting Excess Food Donation to Nonprofit Organizations. (JUN 2020) ([42 U.S.C. 1792](#)). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(X) [52.232-40](#), Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) ([31 U.S.C. 3903](#) and [10 U.S.C. 3801](#)). Flow down required in accordance with paragraph (c) of [52.232-40](#).

(Y) [52.247-64](#), Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) ([46 U.S.C. 55305](#) and [10 U.S.C. 2631](#)). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

I.2.3 FAR 52.217-8 OPTION TO EXTEND SERVICES (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 *100 days*.

I.2.4 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 *90 days*; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least *120 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 *60 months*

I.2.5 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the clause.

(b) The use in this solicitation or contract of any Health and Human Services Acquisition Regulations (48 CFR Chapter 3) clause with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

I.3 HHSAR CLAUSES IN FULL TEXT

I.3.1 352.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—

Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where—

(1) A person other than an authorized user accesses or potentially accesses personally identifiable information, or

(2) An authorized user accesses personally identifiable information for an other than authorized purpose.

Business associate (see 45 CFR 160.103), except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who -

(1) On behalf of such covered entity or of an organized health care arrangement (as defined in this clause) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this contract or agreement, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at [42 CFR 3.20](#), billing, benefit management, practice management, and repricing; or

(2) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR section [164.501](#)), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(3) A covered entity may be a business associate of another covered entity.

(4) Business associate includes the following:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(5) Business associate does not include:

- (i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
- (ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR [164.504\(f\)](#) apply and are met.
- (iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
- (iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Business associate agreement means the agreement, or other arrangement, as dictated by the HIPAA Privacy Rule (45 CFR 160), between an HHS covered entity and a business associate, which must be entered into in addition to the underlying contract for services and before any disclosure (see 45 CFR 160.103) of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of an HHS entity.

Controlled unclassified information (CUI) means information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.

Healthcare component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 CFR 164.105(a)(2)(iii)(D) (see 45 CFR 164.103). The Secretary of HHS has designated HHS as a covered entity (further designated as a “hybrid entity”), and has also designated four HHS divisions as healthcare components under HIPAA, including —

- (1) The Centers for Medicare and Medicaid Services (CMS), insofar as it operates the fee-for-service Medicare program;
- (2) The Program Support Center (PSC), Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers;
- (3) The World Trade Center (WTC) Health Program; and,
- (4) The Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions.

HHS Information Technology General Rules of Behavior means a set of HHS rules that describes the responsibilities and expected behavior of users of HHS information or information systems.

HHS sensitive information means all HHS data, on any storage media or in any form or format, which requires confidentiality, integrity, and availability protection due to the risk of harm that could result to interests of HHS, other agencies or entities, or individuals from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes—

(1) Information where the improper use or disclosure could adversely affect the ability of HHS to accomplish its mission, i.e., HHS proprietary information;

(2) Records about individuals requiring protection under laws and regulations such as the E-Government Act, Privacy Act and the HIPAA Privacy Rule, or based on a data use agreement or a promise or assurance of confidentiality; and

(3) Information that would be exempt from disclosure if requested under the Freedom of Information Act. Examples of HHS sensitive information include—

(i) Individually-identifiable medical, benefits, and personnel information;

(ii) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, security-sensitive, procurement-sensitive, investigatory, and law enforcement information;

(iii) Controlled unclassified information;

(iv) Information that would be confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and

(v) Other information which, if released, could result in a violation of law or agreement, could cause harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

HIPAA Rules means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and part 164.

Incident means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

Information technology (see FAR 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts that include services (including support services), and related resources for information technology.

Organized health care arrangement (see 45 CFR 160.103) means:

- (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
- (2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

- (i) Hold themselves out to the public as participating in a joint arrangement;

and

- (ii) Participate in joint activities that include at least one of the following:

- (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

- (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

- (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

- (3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

- (4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

- (5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Privacy officer means the HHS official(s) with responsibility for implementing and oversight of privacy related policies and practices that impact a given HHS acquisition.

- (b) General. Contractors, subcontractors, their employees, third-parties, and business associates with access to HHS information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to the HHS Cybersecurity Program and the directives and handbooks, complete HHS security training prior to accessing

HHS information (including HHS sensitive information and information systems security and privacy) and on an annual basis thereafter, as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, HHS Personnel Security and Suitability Program, which establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards, and guidance for protecting HHS information, information systems (see 302.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.

(c) Access to HHS information and HHS information systems.

(1) Contractors are limited in their request for logical or physical access to HHS information or HHS information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery, or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with HHS information are subject to the same investigative requirements as those of HHS appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors to access HHS information and HHS information systems shall be in accordance with HHS Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) 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, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be –

(i) Marked appropriately;

(ii) Disclosed to authorized personnel on a need-to-know basis;

(iii) Protected in accordance with NIST SP 800-53, Security and Privacy Controls for 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

(iv) Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

(5) HIPAA business associate agreements. Under the HIPAA Privacy and Security Rules (see 45 CFR 164), pursuant to 45 CFR 164.502(e)(1), a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor of a covered entity's business associate. Additionally, a business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with 45 CFR 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. The satisfactory assurances required by 45 CFR 45 CFR [164.504\(e\)\(1\)](#) of this section shall be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of 45 CFR [164.504\(e\)](#). The contracts shall also include breach reporting policies and procedures for suspected or confirmed breaches of protected health information. The contract shall impose a duty to cooperate with the healthcare component and/or HHS breach investigation and response and must require all subcontractors to comply with the same HIPAA Rules requirements as a condition of receiving government data.

(i) Contractors or entities required to execute business associate agreements for contracts and other agreements become HHS business associates. Business associate agreements are issued by HHS or may be issued by other HHS programs in support of HHS. The HIPAA Privacy Rule requires HHS to execute compliant business associate agreements with persons or entities that create, receive, maintain, or transmit HHS PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of HHS. There may be other HHS components or staff offices which also provide certain services and support to HHS and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to HHS, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a business associate agreements.

(ii) Business associate agreement flow down to subcontractors. A prime contractor required to execute a business associate agreement shall also obtain a satisfactory assurance, in the form of a business associate agreement, of its subcontractors who will also create, receive, maintain, or transmit PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA Rules requirements to the same degree as the Contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits PHI or that will store, generate, access, exchange, process, or utilize such PHI under a contract or agreement is required

to execute a business associate agreement with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to PHI that is required of the covered entity and the prime contractor.

(d) Contractor operations required to be in United States. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other HHS policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable business associate agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information System Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) Roster of employees. Contractors and subcontractors shall provide a roster containing the name, position, e-mail address, phone number, and responsibilities of each employee, including subcontractors, performing work under the contract to develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to Contracting Officer within five (5) business days from the effective date of the contract. Revisions to the roster as a result of staffing changes must be submitted within the number of days of the change provided by the Contracting Officer. The Contracting Officer, or the Contracting Officer's Representative (COR), will notify the Contractor of the appropriate level of investigation required for each staff member based on the information provided on the roster. If an employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.

(f) Contractor/subcontractor employee reassignment and termination notification. Contractors and subcontractors shall provide written notification to the Contracting Officer and COR immediately, and not later than four (4) hours, when an employee working on an HHS information system or with access to HHS information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant HHS contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(g) Non-disclosure agreement. The Contractor and subcontractors shall submit completed non-disclosure agreements, as provided by the Contracting Officer, for each employee having access to non-public government information under this contract. The non-disclosure agreements shall be submitted to the Contracting Officer prior to the performance of work.

(h) HHS information custodial requirements. (1) Release, publication, and use of data. Information made available to a Contractor or subcontractor by HHS for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and

shall not be used in any other way without HHS prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in 52.227-14, Rights in Data—General, paragraph (d).

(2) Media sanitization. HHS information shall not be co-mingled with any other data on the Contractor/subcontractor's information systems or media storage systems in order to ensure federal and HHS requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see [HHS Cybersecurity Program](#)). HHS reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and HHS requirements. The Contractor and subcontractor will provide all necessary access and support to HHS and/or GAO staff during periodic control assessments or audits.

(3) Data retention, destruction and contractor self-certification. The Contractor and its subcontractors are responsible for collecting and destroying any HHS data provided, created, or stored under the terms of this contract, to a point where HHS data or materials are no longer readable or reconstructable to any degree, in accordance with NIST SP 800- 88, Guidelines for Media Sanitization, or subsequent directive. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction or return of all HHS data in its possession accordance with contract requirements or Contracting Officer instructions for disposition, including compliance with National Institute of Standards and Technology (NIST) SP 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) Return of HHS data and information. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the HHS (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying business associate agreement. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract using HHS-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or equipment will be destroyed unless done in accordance with the terms of this contract and the [HHS Agency Records Control Schedules \(2019\)](#).

(5) Use of HHS data and information. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of HHS information only in compliance with the

terms of the contract and applicable Federal and HHS information confidentiality and security laws, regulations, and policies. If Federal or HHS information confidentiality and security laws, regulations, and policies become applicable to the HHS information or information systems after execution of the contract, or if the NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) Copying HHS data or information. The Contractor/subcontractor shall not make copies of HHS information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) Violation of information custodial requirements. If HHS determines that the Contractor has violated any of HHS information confidentiality, privacy, or security provisions, it shall be sufficient grounds for HHS to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) Encryption. The Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract, using cryptography, HHS encryption policies, and HHS-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) Firewall and web services security controls. The Contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed HHS minimum requirements. HHS Configuration Standards Guidelines are available upon request.

(10) Disclosure of HHS data and information. Except for uses and disclosures of HHS information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose HHS information only in two other situations: (i) subject to paragraph 10 of this section, in response to a court order from a court of competent jurisdiction, or (ii) with HHS prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, HHS information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose HHS information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of HHS, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name

and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated HHS facility Privacy Officer as provided in the contract, business associate agreement, or by the Contracting Officer. If providing the Accounting of disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose HHS information protected by any of HHS privacy statutes or applicable regulations including, but not limited to, the Privacy Act of 1974 or the HIPAA Rules. If the Contractor/subcontractor is in receipt of a court order or other requests for HHS information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(i) Compliance with identification policies. Contractors shall comply with the Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; OMB M-19-17; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; HHS Policy for Information Security and Privacy Protection (IS2P) Control Catalog, and Executive Order 13467, Part 1, section 1.2.

(j) Report of known or suspected incident or breach. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of a known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than 7 calendar days as required by Department of Health and Human Services (HHS)/Office of Chief Information Officer (OCIO) [policies](#) and in accordance with supplemental requirements inserted in the contract. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within one week of being notified.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS

Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–Security and Privacy Language.

(k) Incident and breach investigation. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(l) Incident and breach notification requirements. (1) The Contractor/subcontractor shall provide notice to HHS of an incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third- party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk

analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

- (i) Nature of the event (loss, theft, unauthorized access).
- (ii) Description of the event, including:
 - (A) Date of occurrence.
 - (B) Date of incident or breach detection.
 - (C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.
 - (D) Number of individuals affected or potentially affected.
 - (E) Names of individuals or groups affected or potentially affected.
 - (F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.
 - (G) Amount of time the data has been out of HHS control.
 - (H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).
 - (I) Known misuses of data containing sensitive information, if any.
 - (J) Assessment of the potential harm to the affected individuals.
 - (K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.
 - (L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.
 - (M) Steps taken in response to mitigate or prevent a repetition of the incident.
- (m) Training. (1) All Contractor employees and subcontractor employees requiring access to HHS information or HHS information systems shall complete the following before being granted access to HHS information and its systems:
 - (i) On an annual basis, successfully complete the HHS Privacy and Information Security Awareness and HHS Information Security Rules of Behavior training.
 - (ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the HHS Information Security Rules of Behavior, relating to access to HHS information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for HHS personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that HHS Information Security Rules of Behavior signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the HHS Information Security Rules of Behavior, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(n) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and business associate agreements, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to HHS information (including HHS sensitive information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts.)

(End of clause)

I.3.2 352.204-72 RECORDS MANAGEMENT (FEB 2024) (DEVIATION)

(a) Applicability. This clause applies to contracts that include Federal records, as defined in paragraph (b).

(b) Definition. As used in this clause—

Federal record means 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. See 44 U.S.C. 3301.

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by Contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with deliverables.

(2) *Recorded information* means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)

(3) *Personal materials* means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)

(c) Requirements.

(1) The 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. chapters 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 Federal records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

(3) In accordance with 36 CFR 1222.32, the Contractor shall maintain all Federal records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

(5) The Contractor shall immediately notify the 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 appropriate personnel are trained to adhere to these contract requirements, and that applicable, administrative, technical,

and physical safeguards are established to ensure the security and confidentiality of information, data, documentary material, Federal records and/or equipment is properly protected. The Contractor shall not remove Federal Records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, Federal records and/or equipment are no longer required, it shall be returned to HHS 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 as otherwise directed by the Contracting Officer. Destruction of Federal records is expressly prohibited unless in accordance with paragraph (c)(4).

(6) The Contractor shall only use Government information technology equipment for purposes specifically authorized by the contract and in accordance with HHS policy.

(7) The Contractor shall not create or maintain any Federal records containing any non-public HHS information that are not specifically authorized by the contract.

(8) 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.

(9) All Contractor employees assigned to this contract handle Federal records are required to take HHS-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) Subcontract flowdown. The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract.

(End of clause)

I.3.3 352.204-73 CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS (FEB 2024) (DEVIATION)

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

Agency access means access to HHS facilities, sensitive information, information systems or other HHS resources.

Applicant means a contractor employee for whom the Contractor applies for an HHS identification card.

Contractor employee means a prime contractor and subcontractor employee who requires agency access to perform work under an HHS contract.

Identification card (or "ID card") means a government issued or accepted

identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by HHS, or a non-PIV card issued by another Federal agency and approved by HHS. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.

Issuing office means the HHS entity that issues identification cards to contractor employees.

Local security servicing organization means the HHS entity that provides security services to the HHS organization sponsoring the contract.

(b) Risk and sensitivity level designations. For contracts requiring access to HHS facilities, sensitive information, information systems or other HHS resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. HHS will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. The position sensitivity designation levels that apply will be identified in the contract. The following risk and sensitivity level designations and associated level of processing are required, and each level includes the prior levels—

- (1) Low risk level: National Agency Check with Written Inquiries (NACI);
- (2) Moderate risk level: Minimum Background Investigation (MBI); and
- (3) High risk level: Background Investigation.

(c) Security clearances. Contractor employees may also be required to obtain security clearances (i.e., Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in HHS will be processed according to the HHS Personnel Security and Suitability Program, HHS Instruction 731-1, and the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

(d) Pre-screening of contractor employees. The Contractor must pre-screen individuals designated for employment under any HHS contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to HHS for agency access. HHS may decline to grant agency access to a contractor employee for reasons including, but not limited to—

- (1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;

(2) Falsification of information entered on forms or of other documents submitted;

(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and

(4) Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

(e) Citizenship status. The Contractor must monitor a non-citizen's continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

(f) Background investigation and adjudication. A contractor employee must have a favorable adjudication of background investigation before HHS will issue an ID card to the contractor employee granting access to HHS facilities, sensitive information, information systems or other HHS resources. HHS may accept favorable adjudications of background investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. HHS may also accept PIV-I (Interoperable) cards issued by an authorized PIV-1 issuer as evidence of identity. A favorable adjudication does not preclude HHS from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before an HHS identification card can be issued. Each Contractor must use the Office of Personnel Management's (OPM) e-QIP system, or successor system identified by HHS, to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COR or Contracting Officer. The HHS Assistant Secretary for Administration, Program Support Center (PSC), or authorized HHS designee, is responsible for adjudicating the suitability of contractor employees.

(g) Agency access denied. Upon contract award, HHS will initiate the agency access procedure for all contractor employees requiring access to HHS facilities, sensitive information, controlled unclassified information, information systems, and other HHS resources for contract performance. HHS may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The Contractor must not provide agency access to contractor employees until the COR or Contracting Officer provides notice of approval, which is authorized only by the PSC, or authorized HHS designee. Where a proposed contractor employee is denied agency access by the Government or, if for any reason a proposed application is withdrawn by the Contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective pre-screening or planning on the part of the Contractor may be considered as part of the Contractor's overall performance evaluation.

(h) Identification card application process. The COR will be the HHS ID card Sponsor and point of contact for the Contractor's application for an HHS ID card. The COR shall review and approve the HHS ID card application before an ID card is issued to the applicant. An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COR may request the issuing office to waive the six-month eligibility requirement when it is in HHS interest for contract performance. The following applies—

(1) PIV card. The applicant must complete an HHS on-line application for a PIV card;

(2) Non-PIV card. The applicant must complete and submit a hard copy of the necessary form(s) to be provided to Contractor by COR/Sponsor) to the COR/Sponsor; and

(3) Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in person to provide two forms of identity source documents in original form to HHS. The identity source documents must come from the list of acceptable documents included in Form F-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

(i) Identification card custody and control. The Contractor is responsible for the custody and control of all forms of government identification issued by HHS to contractor employees for access to HHS facilities, sensitive information, information systems and other HHS resources. The Contractor shall:

(1) Provide a listing of personnel for whom an identification (ID) card is requested to the COR who will provide a copy of the listing to the card issuing office. This may include Contractor and subcontractor personnel. Follow issuing office directions for submittal of an application package(s).

(2) While visiting or performing work on an HHS facility, as specified by the issuing office or COR, ensure that contractor employees prominently display their ID card.

(3) Immediately notify the COR or, if the COR is unavailable, the Contracting Officer when a contractor employee's status changes and no longer requires agency access (e.g., employee's transfer, completion of a project, retirement, removal from work on the contract, or termination of employment) that may affect the employee's eligibility for access to the facility, sensitive information, or resources.

(4) Promptly deliver to the issuing office: (a) all ID cards assigned to an employee who no longer requires access to the facility; and (b) all expired ID cards within five (5)

days of their expiration or all cards at time of contract termination, whichever occurs first.

(5) Immediately report any lost or stolen ID cards to the issuing office and follow its instructions.

(i) The Contractor is responsible for maintaining and safeguarding the HHS ID card upon issuance to the contractor employee. The Contractor must ensure that contractor employees comply with HHS requirements concerning the renewal, loss, theft, or damage of an ID card. The Contractor must immediately notify the COR or, if the COR is unavailable, the Contracting Officer when an ID card is lost, stolen or damaged.

(ii) Failure to comply with the requirements for custody and control of HHS ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to HHS facilities, sensitive information, information systems or other HHS resources.

(iii) Specific actions and activities are required in certain events—

(A) Renewal. A contractor employee's HHS issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

(B) Lost/stolen. Immediately upon detection, the Contractor or contractor employee must report a lost or stolen HHS ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local servicing security organization. The Contractor must submit an incident report within 48 hours, through the COR or, if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The Contractor must also report a lost or stolen PIV card through the HHS on-line registration system. If the loss or theft is reported by the Contractor to the local police, a copy of the police report must be provided to the COR or Contracting Officer. From the date of notification to HHS, the Contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

(C) Replacement. An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

(D) Surrender of ID cards. Upon notification that routine access to HHS facilities, sensitive information, information systems or other HHS resources is no longer required, the Contractor must surrender the HHS issued ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization in accordance with agency procedures.

(j) Flow down of clause. The Contractor is required to include this clause in any subcontracts at any tier that require the subcontractor or subcontractor's employees to have access to HHS facilities, sensitive information, information systems or other resources.

(End of clause)

I.3.4 352.224-70 NOTIFICATION OF SYSTEM OF RECORDS NOTICE (FEB 2024) (DEVIATION)

(a) This contract provides for the design, development, or operation of a system of records about individuals from which information about an individual is retrieved by the individual's name or by some other identifying particular assigned to the individual.

(b) The System of Records Notice(s) (SORN(s)) that is applicable to this contract is/are: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

Vendor will have access to the following Privacy Act records: Payroll and personnel records about HHS Commissioned Corps personnel.

(c) The System of Records design, development, or operation work the Contractor is to perform is: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

09-40-1402 HHS Payroll Records, 80 FR 48538 (8/13/15), updated at 83 FR 6591 (2/14/18).

09-40-0001 Public Health Service (PHS) Commissioned Corps General Personnel Records, 63 FR 68596 - PDF (12/11/98), updated at 83 FR 6591 (2/14/18).

(d) The disposition to be made of the Privacy Act records upon completion of contract performance is as follows: see "Requirements for Procurements Involving Privacy Act Records" in Section C.

The solicitation and award will state that, at the end of contract performance, OASH CCHQ will provide disposition instructions to the contractor for securely transferring or destroying (in accordance with NIST SP 800-88) any agency records that are in the contractor's (or any subcontractor's) custody or control.

(e) Subcontract flow down. The Contractor is required to include this clause in all subcontracts at any tier performing work under the prime contract involving design, development, or operation work involving a System of Records.

(End of clause)

I.3.5 352.224-71 CONFIDENTIAL INFORMATION (FEB 2024) (DEVIATION)

(a) Definition. As used in this clause—

Confidential information means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) Identification of information. Specific confidential information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, is identified in this contract.

(c) Disclosure. The Contractor shall not disclose confidential information or records written notice is provided to the Contracting Officer at least 45 days in advance of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency. The Contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.

(d) Government furnished or provided information: For information provided by or on behalf of the government—

(1) The publication or dissemination of the following types of information are restricted under this contract: **To Be Determined**

(2) The reason(s) for restricting the types of information identified in subparagraph (d)(1) is/are:

_____.

(e) The Contractor shall consult with the Contracting Officer when there is uncertainty with regard to the confidentiality of, or a property interest in, information under this contract prior to the release, disclosure, dissemination, or publication of such information.

(End of clause)

I.3.6 HHSAR 352.239-70 STANDARDS FOR HEALTH INFORMATION TECHNOLOGY (DEC 2022) (DEVIATION)

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

Health information technology (health IT) means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. (42 U.S.C. 300jj)

Individually identifiable health information means information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health condition of an

individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (42 U.S.C. 300jj, 1320d)

ONC Health Information Technology Certification Program means the certification program administered by the HHS Office of the National Coordinator for Health Information Technology (ONC) using a third-party conformity assessment program for health IT. Certification criteria for the Program, which incorporate standards and implementation specifications in 45 CFR part 170 subpart B, are found in 45 CFR part 170, subpart C.

(b) Pursuant to the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. 111-5, Title XIII, sections 13111 and 13112, by submission of an offer and execution of a contract, the Contractor agrees that—

(1) For any work performed under the contract that involves implementing, acquiring, or upgrading health IT used for the direct exchange of individually identifiable health information between agencies and with non-Federal entities, the Contractor will utilize health IT that—

(i) Meets standards and implementation specifications adopted in 45 CFR part 170, subpart B, if such standards and implementation specifications can support the work performed under the contract; and

(ii) Is certified under the ONC Health Information Technology Certification Program, if certified technology can support the work performed under the contract (see certification criteria in 45 CFR part 170, subpart C), when the Contractor is an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act, or when the Contractor is implementing, acquiring or upgrading technology to be used by an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act.

(2) If the Contractor is a health care provider, health plan, or health insurance issuer, or is establishing an agreement with a health care provider, health plan, or health insurance issuer, for work performed under the contract that involves implementing, acquiring, or upgrading health IT, the Contractor will utilize health IT that—

(i) Meets standards and implementation specifications adopted in 45 CFR part 170, subpart B, if such standards and implementation specifications can support the work performed under the contract; and

(ii) Is certified under the ONC Health Information Technology Certification Program, if certified technology can support the work performed under the contract (see certification criteria in 45 CFR part 170, subpart C), when the Contractor is an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act, or when the Contractor is implementing, acquiring or upgrading technology to be used by an eligible professional in an ambulatory setting, or a hospital, eligible under sections 4101, 4102 and 4201 of the HITECH Act.

(c) If standards and implementation specifications adopted in 45 CFR part 170, subpart B, cannot support the work as specified in the contract, the Contractor is encouraged to use health IT that meets non-proprietary standards and implementation specifications developed by consensus-

based standards development organizations. This may include standards identified in the ONC Interoperability Standards Advisory, available at <https://www.healthit.gov/isa/>.
(End of clause)

I.3.7 352.239-71 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—

Information technology has the same meaning in FAR 2.101.

Information and communication technology (ICT) also means information technology (see FAR 2.101 for definitions).

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) Responsibilities. The Contractor shall be responsible for information technology security for all systems connected to a Department of Health and Human Services (HHS) network or operated by the Contractor for HHS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to HHS information that directly supports the mission of HHS. Examples of tasks that require security provisions include—

(1) Hosting of HHS e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by HHS with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to HHS general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) Information system security plan. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. HHS information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, privacy impact assessment (PIA), system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and the system privacy plan, as determined by the Contracting Officer's Representative. The plan shall address the specific contract requirements regarding information systems or related support or

services included in the contract, to include the PWS or SOW. The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information technology security requirements in accordance with Federal and HHS policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following:

- (1) OMB Circular A-130, Managing Information as a Strategic Resource;
 - (2) National Institute of Standards and Technology (NIST) Guidelines;
 - (3) Federal Information Processing Standard (FIPS) 200; and
 - (4) HHS Cybersecurity Program related to HHS information (including HHS sensitive information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, the Cyber Security Checklist and Cyber Security Infographic at <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>, which provides HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting HHS information, information systems (see 302.101, Definitions), information technology, and ICT, security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.
- (d) Submittal of plan. Within 60 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.
- (e) Authority to Operate (ATO). As required by current HHS policy, the Contractor shall submit written proof of information technology security accreditation with a valid ATO to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with HHS policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this ATO a final security plan, risk assessment, security test and evaluation, privacy threshold analysis or privacy impact assessment, and a disaster recovery plan/continuity of operations plan.
- (f) Annual validation. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.
- (g) Banners. The Contractor shall ensure that the official HHS banners are displayed on all HHS systems (both public and private) operated by the Contractor that contain Privacy Act or other sensitive information before allowing anyone access to the system. The Office of Information Technology will make official HHS banners available to the Contractor.
- (h) Screening and access. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for HHS or interconnected to an HHS network in accordance with HHS policies referenced in paragraph (c).

(i) Training. The Contractor shall ensure that its employees performing services under this contract complete HHS security awareness and privacy training on an annual basis. This includes signing an acknowledgment on an annual basis that they have read, understand, and agree to abide by the HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy as required; FAR 39.105, Privacy; clause 352.204-71, Information and Information Systems Security, and this clause.

(j) Government access. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information systems, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information technology inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of HHS data or to the function of information technology systems operated on behalf of HHS), and to preserve evidence of computer crime.

(k) Notification of termination of employees. The Contractor shall immediately notify the Contracting Officer when an employee who has access to HHS information systems or data terminates employment.

(l) Subcontract flow down requirement. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

I.3.8 352.239-73 INFORMATION SYSTEM DESIGN AND DEVELOPMENT (FEB 2024) (DEVIATION)

(a) Design or development at non-HHS facilities. Information systems that are designed or developed for or on behalf of HHS at non-HHS facilities shall comply with all HHS directives developed in accordance with the Federal Information Security Modernization Act of 2014, Health Insurance Portability and Accountability Act (HIPAA) regulations, National Institute of Standards and Technology (NIST), and related HHS security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR Part 164, Subpart C, information and system security categorization level designations in accordance with Federal Information Processing Standards (FIPS) 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections Reference Architecture.

(b) Privacy Impact Assessment. During the development cycle a Privacy Impact Assessment must be completed by the contractor, provided to the Contracting Officer Representative, and approved by the appropriate HHS and Operating Division security and privacy officials; government, contractor, or independent third party.

(c) Security of procured or developed systems and technologies. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that security fixes shall not negatively impact the Systems.

(d) Subcontract flow down requirements. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts where services to perform information system design and development are required.

(End of clause)

I.3.9 352.239-74 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—

Assessment and Authorization (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable HHS policies and procedures is the mechanism by which HHS provides an Authorization to Operate (ATO), the official management decision given by the HHS to authorize operation of an information system.

Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

(b) Hosting, operation, maintenance, or use at non-HHS facilities. For information systems that are hosted, operated, maintained, or used on behalf of HHS at non-HHS facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required HHS confidentiality statutes included in HHS mandatory yearly training and privacy policy, Federal Information Security Modernization Act (FISMA), National Institutes of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and HHS security and privacy policy. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security and privacy control procedures must be equivalent to or exceed, those procedures used to secure HHS systems. A Privacy Impact Assessment (PIA) (if the system includes Personally Identifiable Information (PII)) or a Privacy Threshold Analysis (to determine if the system includes PII) must also be provided to the Contracting Officer Representative

(COR) and approved by HHS Senior Agency Official for Privacy (SAOP) or designee prior to ATO. All external Internet connections to HHS network involving HHS information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and reviewed and approved by HHS prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) Collecting, processing, transmitting, and storing of PII. Adequate security and privacy controls for collecting, processing, transmitting, and storing of PII, as determined by the HHS SAOP or designee, must be in place, tested, and approved by HHS prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of HHS. These security and privacy controls are to be assessed and stated within the PIA, Information System Security Plan, Information System Privacy Plan, Security Control Assessment Report, and/or Privacy Control Assessment Report, as agreed upon by the Contractor, COR, and the Operating Division Senior Official for Privacy. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

(d) Annual FISMA security controls assessment. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into HHS Plan of Action & Milestones (POA&M) management process. The Contractor/subcontractor must use HHS POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the HHS in the performance work statement or statement of work, or in the approved remediation plan through the HHS POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by HHS officials, including the HHS Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy. Major changes introducing new privacy risks require an updated and reapproved PIA.

(e) Annual self-assessment. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. HHS reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing,

at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.

(f) Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on HHS networks. HHS prohibits the installation and use of personally-owned or Contractor/subcontractor-owned equipment or software on HHS networks. If non-HHS owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, performance work statement, statement of work, or contract. All of the security controls required for government furnished equipment must also be utilized in approved other equipment (OE) at the

Contractor's expense. All remote systems must be equipped with, and use, an HHS- approved antivirus software and a personal (host-based or enclave based) firewall that is configured with an HHS-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-HHS owned OE.

(g) Disposal or return of electronic storage media on non-HHS leased or non-HHS owned IT equipment. All electronic storage media used on non-HHS leased or non-HHS owned IT equipment that is used to store, process, or access HHS information must be handled in adherence with disposition instructions upon—

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (e.g., hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain HHS information must be returned to the HHS for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per disposition instructions. This must be completed within 30 days of termination of the contract.

(h) Bio-Medical devices and other equipment or systems. Bio-Medical devices and other equipment or systems containing media (e.g., hard drives, optical disks) with HHS sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of HHS sensitive information the devices may be provided back to the Contractor under one of three scenarios—

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn- in if HHS initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

I.3.10 352.239-75 SECURITY CONTROLS COMPLIANCE TESTING (FEB 2024)
(DEVIATION)

On a periodic basis, HHS, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein HHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of HHS, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by HHS in the event of an incident or a breach, or at any other time.

(End of clause)

I.3.11 352.239-76 SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED
CONTRACTOR-OPERATED AND CONTRACTOR-OWNED CONTRACTOR- OPERATED
RESOURCES (FEB 2024) (DEVIATION)

(a) Federal policies. The Contractor shall comply with applicable federal laws, regulations, and HHS policies that include, but are not limited to—

- (1) HHS Policy for Information Security and Privacy Protection (IS2P);
- (2) Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101);
- (3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, Security and Privacy Controls for Information Systems and Organizations;
- (4) Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and
- (5) Any other applicable federal laws, regulations, NIST guidance, and local HHS policies.

(b) Assessment and Authorization (A&A). A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) of 30 business days post contract award. The Contractor must conduct the A&A requirements in accordance with [HHS IS2P](#), NIST SP 800-37, Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach (latest revision), NIST SP 800-53B, Control Baselines for Information Systems and Organizations, and the NIST SP 800-53A (latest revision). HHS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented

and operating effectively.

(1) A&A package deliverables. The Contractor shall provide an A&A package within timeline, process, and format as determined and required by the HHS and FedRAMP A&A Guidelines to the Contracting Officer and/or the Contracting Officer's Representative (COR). The following A&A deliverables are required to complete the A&A package— No required deliverables.

(ii) A System Security Plan (SSP) is due to the CO and COR within 60 days following the start of the contract's period of performance. The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system (see HHSAR 302.101, Definitions) as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall review and update the SSP at least **annually** thereafter and if requested, provide a copy of the updated SSP to the COR.

(iii) A Security Assessment Plan/Report (SAP/SAR) is due to the CO/COR within two weeks following the start of the contract period of performance. The security assessment must be conducted by independent assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with the COR shall conduct, or as directed, in the assessment of the security controls within two weeks following the contract period of performance and updated the SAR at least **annually**. A copy of the updated SAR shall be provided to the COR, if requested.

(iv) All systems shall have a completed privacy threshold analysis (PTA). If the PTA results determines the system contains personally identifiable information, a privacy impact assessment, approved by the HHS SAOP, is required.

(v) System Privacy Plan and Privacy Control Assessment. As required in OMB Circular A-130, a System Privacy Plan and Privacy Control Assessment shall be included in A&A. The plan and assessment may be included in the Security System Plan, or a separate report in the A&A, as determined by the COR.

(vi) An Independent Assessment is due to the CO and COR within 30 business days following the start of the contract's period of performance. The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party shall review and analyze the security authorization package and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address

all "high" deficiencies before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).

(vii) The POA&M is due as follows—

(A) to the CO and COR within two weeks following the start of the contract's period of performance. OS will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor(s) for mitigating in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and HHS/OS policies. Depending on the severity of the risks, OS may require designated POA&M weakness to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses through the contract. As required by HHS/OCIO [policies](#) and in accordance with supplemental requirements inserted in the contract, from the date the weaknesses are formally identified and documented;

(B) Critical-risk weaknesses must be mitigated within fifteen (15) days from the date the weaknesses are formally identified and documented;

(C) High-risk weaknesses must be mitigated within thirty (30) days from the date the weaknesses are formally identified and documented;

(D) Medium weaknesses must be mitigated within ninety (90) days from the date the weaknesses are formally identified and documented; and

(E) Low weaknesses must be mitigated within three hundred and sixty-five days (365) from the date the weaknesses are formally identified and documented.

(2) HHS will determine the risk rating of all vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones policies. Depending on the severity of the risks, HHS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document shall be updated at least quarterly.

(3) A Contingency Plan and Contingency Plan Test are due to the CO and COR within 30 business days post contract award. The Contingency Plan shall be developed in accordance with NIST SP 800-34, Contingency Planning Guide for Federal Information Systems, and be consistent with HHS policies. Upon final acceptance by the System Owner, the Contractor, in coordination with the COR and System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned, and any remaining action items to be addressed. The Contractor shall update and test the Contingency Plan at least ***annually***.

(4) An E-Authentication Questionnaire is required. The Contractor shall collaborate with at the COR's direction to ensure that the E-Authentication Guidance requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 series, latest versions. Based on the level of assurance determined by the E-Authentication, the Contractor shall ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E- Authentication (when required), in accordance with HHS Guidance for Selection of e- Authentication Assurance Levels and any other applicable HHS policies.

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

(6) Annual assessment/penetration (pen) test. The Contractor shall assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by the specified due date provided by the COR.

(7) Asset management. Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, the Contractor shall provide an inventory of all information technology (IT) assets for hardware and software (computers, servers, routers, databases, operating systems, etc.) that are processing HHS- owned information and/or data. It is anticipated that this inventory information will be required to be produced at least within two weeks following the start of the contract's period of performance. IT asset inventory information shall include—

(i) IP address;

(ii) Machine name;

(iii) Operating system level;

(iv) Security patch level; and

(v) SCAP-compliant format information. The Contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the HHS Policy for Information Technology Asset Management (ITAM) and any other applicable HHS policy.

(8) Configuration management. The Contractor shall use available SCAP- compliant automated tools as per NIST IR 7511 and HHS Minimum Security Configurations Standards Guidance to scan all IT assets, including but not limited to computers, servers, routers, databases, operating

systems, application, etc., that store and process government information. The Contractor shall provide scan reports to the COR upon request. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

(9) Vulnerability management. The Contractor shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS Policy for Vulnerability Management. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least annually.

(10) Patching and vulnerability remediation. The Contractor shall install vendor- released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

(11) Secure coding. The Contractor shall follow the HHS Policy for Software Development Secure Coding Practices and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team specified standards, the Software Engineering Institute (SEI) CERT and the Open Web Application Security Project, that will limit system software vulnerability exploits.

(12) Boundary protection. The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection.

(13) Government access for security assessment.

(i) In addition to the Inspection Clause in the contract, the Contractor shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS. This access includes, but is not limited to—

(1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, access to Contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. For the purposes of this paragraph only, Government includes, but is not limited to, Contracting Officer, COR, the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of

access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include, but not be limited to, such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, Structured Query Language injection vulnerabilities, and any other known vulnerabilities.

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

(ii) The Contractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Government inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

(iii) The Contractor shall cooperate with inspections, audits, investigations, and reviews.

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

(d) Desktops, laptops, and other computing devices required for use by the Contractor. The Contractor shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

(1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program.

(2) Configure laptops and desktops in accordance with the latest applicable United States

Government Configuration Baseline, and HHS Minimum Security Configuration Standards.

(3) Maintain the latest operating system patch release and anti-virus software definitions at least within one week of notice.

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

(5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

(i) Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

(ii) Using SCAP-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the Contracting Officer and/or COR, Project Officer, and any other point of contact designated by the Contracting Officer or COR.

(e) Rights to data. Contractors shall specify any data rights asserted and mark such deliverables accordingly in accordance with applicable data rights clauses set forth in the contract.

(f) Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements. The Contractor shall secure their ICT supply chain in compliance with HHS Policy for Cyber Supply Chain Risk Management and Public Law 115-232, section 889. At a minimum, the Contractor shall—

(1) Develop rules for suppliers' development methods, techniques, or practices;

(2) Use secondary market components;

(3) Prohibit counterfeit products;

(4) Dispose and/or retain elements such as components, data, or intellectual property securely;

(5) Ensure adequate supply of components;

(6) Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;

(7) Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;

(8) Establish Service Level Agreements (SLAs), patching vehicles, and disclosure requirements in the case of an incident or new vulnerability being discovered; and

(9) Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and

(10) Prohibit the use of covered telecommunications and video surveillance equipment or services.

(g) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts and third-party agreements, at any tier, of any amount and in which subcontractor employees and third-party servicers/employees, will perform functions or provide products under the scope of this contract, and have access to HHS information (including HHS sensitive information, i.e., protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101, Definitions).

(End of clause)

I.3.12 352.239-77 CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION)

(a) Responsibilities. This clause is applicable to all or any part of the contract that includes cloud computing services. The Contractor shall be responsible for the following privacy and security requirements on this contract—

(1) Federal Risk and Authorization Management Program (FedRAMP) compliant authorization to operate. Compliance with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service (see HHSAR 302.101, Definitions) under this contract has an approved FedRAMP compliant authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO within the first two weeks following the start of the contract's period of performance.

(i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at [fedramp.gov](https://www.fedramp.gov)). The HHS Policy for Information Security and Privacy Protection (IS2P) and HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance further define the baseline policies as well as roles and responsibilities. The Contractor shall implement additional controls identified by the agency in this contract.

(ii) A security control assessment must be conducted by a FedRAMP third- party assessment organization (3PAO) for the initial ATO and annually thereafter, or when there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

(2) Data jurisdiction. The Contractor shall store all information within the security authorization boundary, data at rest, or data backup, within the Continental United States.

(3) Service Level Agreements (SLAs). When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and

the cloud service provider and work with the Contracting Officer's Representative (COR) to develop and maintain an SLA, as provided in the contract.

(4) Interconnection Agreements/Memorandum of Agreements. When applicable and identified in this contract, the Contractor shall establish and maintain interconnection agreements and or memorandum of agreements/understanding in accordance with HHS policies.

(b) Protection of information in a cloud environment.

(1) If Contractor personnel shall remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS policies, available at <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.

(2) HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS and hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data shall be made available to HHS, at no additional cost, within one (1) business day from the date of the request, or within the timeframe otherwise specified.

(3) The Contractor shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

(4) The Contractor shall comply with NARA-approved records schedule(s) and protection requirements for federal agency electronic records in accordance with 36 CFR 1236.20 and 1236.22 (ref. a), including but not limited to —

(i) Maintenance of links between records and metadata; and

(ii) Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

(5) The disposition of all HHS data shall be at the written direction of the COR. This may include documents returned to HHS control, destroyed, or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(i) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements in accordance with HHSAR 352.224-70, FAR 52.224-1 and 52.224-2: HHSAR "Confidential Information" clause, 352.224-71.

(c) Assessment and Authorization (A&A) process.

(1) The Contractor shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, privacy policies, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS security policies.

Certification must be completed in the timeframe required under HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance.

(i) In addition to the FedRAMP compliant ATO, the Contractor shall complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation. Additional requirements and completion/submission timelines: See HHS Policy for Information Security and Privacy Protection (IS2P), HHS Policy for Information Security and Privacy Protection (IS2P Control Catalog, HHS Policy for Information Technology (IT) Policy for Enterprise Performance Life Cycle (EPLC). The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.

(ii) Cloud Service Provider (CSP) systems categorized as FIPS 199 High, Moderate or Low are recommended but not required to leverage a FedRAMP accredited Third Party Assessment Organization (3PAO). A CSP's agency partner may choose to use their own Independent Verification and Validation (IV&V) organization or 3PAO to assess the system. If an agency chooses to use their own IV&V team or an unaccredited 3PAO, they must submit an attestation regarding the team's independence to the agency and the FedRAMP PMO, and the IV&V / 3PAO team must use FedRAMP templates for the assessment and follow all FedRAMP requirements.

(iii) For all cloud services, the A&A package must contain the following documentation/package deliverables:

System Security Plan (SSP), Security Assessment Report (SAR), POA&M, Configuration Management Plan (CMP), Contingency Plan (CP) and Contingency Plan Test (CPT) Report, E-Auth (if applicable), PTA/PIA (if applicable), Service Level Agreement, Authorization Letter, Configuration Management Plan (if applicable), and Configuration Baseline.

(iv) Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with HHS policies. The following templates and timelines are applicable:

The contractor shall use the FedRAMP template (<https://www.fedramp.gov/>). Deliverable timelines will be determined by FedRAMP guidance.

(2) HHS reserves the right to perform penetration testing on all systems operated on behalf of the agency. If the Contracting Officer exercises this right, the Contractor shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS requirements. Review activities include, but are not limited to—

- (i) Scanning operating systems, web applications, wireless scanning;
 - (ii) Network device scanning to include routers, switches, and firewall, and IDS/IPS; and,
 - (iii) Databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
- (3) The Contractor shall identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the Contractor's expense before HHS issues an ATO.
- (4) The Contractor shall mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings shall be remediated in accordance with timelines specified in the HHS POA&M Standard from discovery—
- (i) Critical vulnerabilities no later than fifteen (15) days;
 - (ii) High within thirty (30) days;
 - (iii) Medium within ninety (90) days; and
 - (iv) Low vulnerabilities no later than three hundred and sixty (360) days, unless otherwise specified.
 - (v) In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines: (1) critical vulnerabilities no later than fifteen (15) days and (2) high vulnerabilities within thirty (30) days, (3) medium vulnerabilities within sixty (60) days, and (4) low vulnerabilities no later than one hundred and eighty (180) days.
- (5) Revocation of a cloud service. HHS has the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information (see HHSAR 302.101, Definitions), HHS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the internet, other networks, or applying additional security controls.
- (d) Reporting and continuous monitoring.

(1) Following the initial ATOs, the Contractor shall perform the minimum ongoing continuous monitoring activities, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. The minimum ongoing continuous monitoring activities include—

Submit required deliverables by the specified due dates, meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, POA&M updates, revised security documentation/Agreements and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. Monitoring activities will include monthly reports/invoices and ad hoc meetings to discuss progress.

(2) At a minimum, the Contractor shall provide the following artifacts/deliverables on a monthly basis using the following process and format: in electronic format via email or uploaded to an approved collaboration tool.

(i) Operating system, database, Web application, and network vulnerability scan results;

(ii) Updated POA&Ms;

(iii) Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO, and;

(iv) Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract shall be approved by the agency.

(e) Configuration baseline.

(1) The Contractor shall certify that applications are fully functional and operate correctly as intended on systems using HHS Minimum Security Configurations Standards Guidance. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS configuration baseline.

(2) The Contractor shall use NIST Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

(f) Report of known or suspected incident or breach. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of an known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than 3 calendar days. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within 3 calendar days.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements— Security and Privacy Language.

(g) Incident and breach investigation. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(h) Incident and breach notification requirements. (1) The Contractor/subcontractor shall provide notice to HHS of a privacy or incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third- party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(i) Media transport.

(1) The Contractor shall be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non- digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

Minimum requirements for media transport: physical removal and transportation of data shall be logged with documented chain of custody form and approved by the OS CISO.

(2) All information, devices and media shall be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

(j) Boundary Protection—Trusted Internet Connections (TIC).

(1) The Contractor shall ensure that government information (other than unrestricted information) being transmitted from Federal government entities to external entities using cloud services is inspected by TIC processes that are in compliance with the requirements of the Office of Management and Budget Memorandum 19-26: Update to the TIC Initiative, TIC 3.0.

(2) The Contractor shall route all external connections through a TIC.

(3) Non-Repudiation. The Contractor shall provide a system that implements encryption with current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program that provides for origin authentication, data integrity, and signer non-repudiation.

(k) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (i), in subcontracts and third-party agreements, of any amount and in which subcontractor employees, and third-party servicers/employees, will perform functions where they will provide cloud computing services and have access to HHS information (including HHS sensitive information, i.e., protected health information (see HHSAR 302.101, Definitions)), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts).

(End of clause)

I.3.13 352.239-79 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2024) (DEVIATION)

Subpart 339.2 (deviated) applies to the acquisition of Information and Communication Technology (ICT) supplies, products, platforms, information, documentation, and services support. It concerns the access to and use of information and data, by both Federal employees with disabilities, and members of the public with disabilities in accordance with FAR 39.201.

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT)

supplies, products, platforms, information, documentation, and services support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at <https://www.access-board.gov/ict/>. Information about Section 508 is available at <https://www.hhs.gov/web/section-508/index.html>.

(b) Additional Section 508 accessibility standards applicable to this contract or order may be identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see <https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see <https://www.itic.org/policy/accessibility/vpat>), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see <https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>) or an ACR (based on the VPAT see <https://www.itic.org/policy/accessibility/vpat>), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of if ythe supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements.

(End of clause)

SECTION J - List of Attachments

Reference Number	Title	Number of Pages
J.1	Past Performance Questionnaire	7
J.2		
J.3		

SECTION K - Representations, Certifications, and Other Statements of Offerors or Respondents

K.1 NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM CODE

(1) The North American Industry classification System (NAICS) code for this acquisition 514214.

(2) The small business size standard is \$39,000,000.00.

K.2 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES. (NOV 2023)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically in the System for Award Management (SAM) accessed through <https://www.sam.gov>. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (v) of this provision.

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

"Covered telecommunications equipment or services" has the meaning provided in the clause [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with [13 CFR part 127](#), and the concern is certified by SBA or an approved third-party certifier in accordance with [13 CFR 127.300](#). It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

- (1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or
- (2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation, means a foreign incorporated entity that meets the definition of

an inverted domestic corporation under [6 U.S.C. 395\(b\)](#), applied in accordance with the rules and definitions of [6 U.S.C. 395\(c\)](#).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

- (1) PSC 5510, Lumber and Related Basic Wood Materials;
- (2) Product or Service Group (PSG) 87, Agricultural Supplies;
- (3) PSG 88, Live Animals;
- (4) PSG 89, Subsistence;
- (5) PSC 9410, Crude Grades of Plant Materials;
- (6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
- (7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
- (8) PSC 9610, Ores;
- (9) PSC 9620, Minerals, Natural and Synthetic; and
- (10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Reasonable inquiry has the meaning provided in the clause [52.204-25](#), Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

- (1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;
- (2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;
- (3) Consist of providing goods or services to marginalized populations of Sudan;
- (4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;
- (5) Consist of providing goods or services that are used only to promote health or education; or
- (6) Have been voluntarily suspended."Sensitive technology"—

Sensitive technology—

- (1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—
 - (i) To restrict the free flow of unbiased information in Iran; or
 - (ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

- (2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

Service-disabled veteran-owned small business concern—

(1) Means a small business concern—

- (i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and
- (ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in [38 U.S.C. 101](#)(2), with a disability that is service connected, as defined in [38 U.S.C. 101](#)(16).

Small business concern—

- (1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation, and qualified as a small business under the criteria in [13 CFR part 121](#) and size standards in this solicitation.
- (2) *Affiliates*, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern, consistent with 13 CFR 124.1001, means a small business concern under the size standard applicable to the acquisition, that—

- (1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—
- (i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and
- (ii) Each individual claiming economic disadvantage has a net worth not exceeding the threshold at 13 CFR 124.104(c)(2) after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and
- (2) The management and daily business operations of which are controlled (as defined at 13 CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

- (1) Directly by a parent corporation; or
- (2) Through another subsidiary of a parent corporation

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

- (1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and
- (2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned business concern means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women

Women-owned small business concern means a small business concern—

- (1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and
- (2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with [13 CFR part 127](#)), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with [13 CFR 127.300](#).

(b)

- (1) *Annual Representations and Certifications*. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.
- (2) The offeror has completed the annual representations and certifications electronically in SAM accessed through <http://www.sam.gov>. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR [52.212-3](#), Offeror Representations and Certifications-Commercial Products and Commercial Services, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard(s) applicable to the NAICS code(s) referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR [4.1201](#)), except for paragraphs ____.

[Offeror to identify the applicable paragraphs at (c) through (v) of this provision that the offeror has completed for the purposes of this solicitation only, if any.

These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on SAM.]

- (c) Offerors must complete the following representations when the resulting contract is for supplies to be delivered or services to be performed in the United States or its outlying areas, or when the contracting officer has applied [part 19](#) in accordance with [19.000\(b\)\(1\)\(ii\)](#). Check all that apply.

- (1) *Small business concern*. The offeror represents as part of its offer that—

- (i) It ☐ is, ☐ is not a small business concern; or

- (ii) It ☐ is, ☐ is not a small business joint venture that complies with the requirements of [13 CFR 121.103\(h\)](#) and [13 CFR 125.8\(a\)](#) and [\(b\)](#). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*]
- (2) *Veteran-owned small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents as part of its offer that it ☐ is, ☐ is not a veteran-owned small business concern.
- (3) *Service-disabled veteran-owned small business concern.* [*Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.*] The offeror represents as part of its offer that—
- (i) It ☐ is, ☐ is not a service-disabled veteran-owned small business concern; or
- (ii) It ☐ is, ☐ is not a joint venture that complies with the requirements of [13 CFR 125.18\(b\)\(1\)](#) and [\(2\)](#). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*] Each service-disabled veteran-owned small business concern participating in the joint venture shall provide representation of its service-disabled veteran-owned small business concern status.
- (4) *Small disadvantaged business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents, that it ☐ is, ☐ is not a small disadvantaged business concern as defined in 13 CFR 124.1002.
- (5) *Women-owned small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents that it ☐ is, ☐ is not a women-owned small business concern.
- (6) *WOSB joint venture eligible under the WOSB Program.* The offeror represents that it ☐ is, ☐ is not a joint venture that complies with the requirements of [13 CFR 127.506\(a\)](#) through [\(c\)](#). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*]
- (7) *Economically disadvantaged women-owned small business (EDWOSB) joint venture.* The offeror represents that it ☐ is, ☐ is not a joint venture that complies with the requirements of [13 CFR 127.506\(a\)](#) through [\(c\)](#). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*]
- Note to paragraphs (c)(8) and (9):** Complete paragraphs (c)(8) and (9) only if this solicitation is expected to exceed the simplified acquisition threshold.
- (8) *Women-owned business concern (other than small business concern).* [*Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents that it ☐ is a women-owned business concern.
- (9) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price: _____
- (10) *HUBZone small business concern.* [*Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.*] The offeror represents, as part of its offer, that—
- (i) It ☐ is, ☐ is not a HUBZone small business concern listed, on the date of this representation, as having been certified by SBA as a HUBZone small business concern in the Dynamic Small Business Search and SAM, and will attempt to maintain an employment rate

- of HUBZone residents of 35 percent of its employees during performance of a HUBZone contract (see [13 CFR 126.200\(e\)\(1\)](#)); and
- (ii) It ☐ is, ☐ is not a HUBZone joint venture that complies with the requirements of [13 CFR 126.616\(a\)](#) through [\(c\)](#). [*The offeror shall enter the name and unique entity identifier of each party to the joint venture: _____.*] Each HUBZone small business concern participating in the HUBZone joint venture shall provide representation of its HUBZone status.
- (d) Representations required to implement provisions of Executive Order 11246-
- (1) Previous contracts and compliance. The offeror represents that-
- (i) It ☐ has, ☐ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and
- (ii) It ☐ has, ☐ has not filed all required compliance reports.
- (2) *Affirmative Action Compliance.* The offeror represents that-
- (i) It ☐ has developed and has on file, ☐ has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or
- (ii) It ☐ has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.
- (e) *Certification Regarding Payments to Influence Federal Transactions* (31 <http://uscode.house.gov/> U.S.C. 1352). (Applies only if the contract is expected to exceed \$150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.
- (f) *Buy American Certificate.* (Applies only if the clause at Federal Acquisition Regulation (FAR) [52.225-1](#), Buy American-Supplies, is included in this solicitation.)
- (1)
- (i) The Offeror certifies that each end product and that each domestic end product listed in paragraph (f)(3) of this provision contains a critical component, except those listed in paragraph (f)(2) of this provision, is a domestic end product.
- (ii) The Offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select "no".
- (iii) The Offeror shall separately list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).

- (iv) The terms “commercially available off-the-shelf (COTS) item,” “critical component,” “domestic end product,” “end product,” “foreign end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American-Supplies.”

(2) Foreign End Products:

Line Item No.	Country of Origin	Exceeds 55% domestic content (yes/no)

[List as necessary]

(3) Domestic end products containing a critical component:

Line Item No. _____

[List as necessary]

- (4) The Government will evaluate offers in accordance with the policies and procedures of FAR [part 25](#).

(g)

- (1) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate*. (Applies only if the clause at FAR [52.225-3](#), Buy American-Free Trade Agreements-Israeli Trade Act, is included in this solicitation.)

(i)

- (A) The Offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (iii) of this provision, is a domestic end product and that each domestic end product listed in paragraph (g)(1)(iv) of this provision contains a critical component.

- (B) The terms “Bahraini, Moroccan, Omani, Panamanian, or Peruvian end product,” “commercially available off-the-shelf (COTS) item,” “critical component,” “domestic end product,” “end product,” “foreign end product,” “Free Trade Agreement country,” “Free Trade Agreement country end product,” “Israeli end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American-Free Trade Agreements-Israeli Trade Act.”

- (ii) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled “Buy American-Free Trade Agreements-Israeli Trade Act.”

Free Trade Agreement Country End Products (Other than Bahraini, Moroccan, Omani, Panamanian, or Peruvian End Products) or *Israeli End Products*:

Line Item No.	Country of Origin

--	--

[List as necessary]

- (iii) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act." The Offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select "no".

Other Foreign End Products:

Line Item No.	Country of Origin	Exceeds 55% domestic content (yes/no)

[List as necessary]

- (iv) The Offeror shall list the line item numbers of domestic end products that contain a critical component (see FAR [25.105](#)).

Line Item No. _____

[List as necessary]

- (v) The Government will evaluate *offers* in accordance with the policies and procedures of FAR [part 25](#).

- (2) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate II.*

If Alternate II to the clause at FAR [52.225-3](#) is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

- (g)(1)(ii) The offeror certifies that the following supplies are Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Israeli End Products:

Line Item No.

[List as necessary]

(3) *Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate III.*

If Alternate III to the clause at [52.225-3](#) is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

- (g)(1)(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahraini, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahraini, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin

[List as necessary]

(4) *Trade Agreements Certificate.* (Applies only if the clause at FAR [52.225-5](#), Trade Agreements, is included in this solicitation.)

- (i) The offeror certifies that each end product, except those listed in paragraph (g)(4)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled "Trade Agreements."
- (ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin

[List as necessary]

- (iii) The Government will evaluate offers in accordance with the policies and procedures of FAR [part 25](#). For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

- (h) *Certification Regarding Responsibility Matters (Executive Order 12689).* (Applies only if the contract value is expected to exceed the simplified acquisition threshold.)

The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals–

- (1) ☐ Are, ☐ are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;
- (2) ☐ Have, ☐ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;
- (3) ☐ Are, ☐ are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and
- (4) ☐ Have, ☐ have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at [9.104-5\(a\)\(2\)](#) for which the liability remains unsatisfied.
 - (i) Taxes are considered delinquent if both of the following criteria apply:
 - (A) *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.
 - (B) *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.
 - (ii) *Examples.*
 - (A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.
 - (B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.
 - (C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.
 - (D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

- (i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126).* [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at [22.1503\(b\)](#).]
- (1) *Listed end products.*

Listed End Product	Listed Countries of Origin

- (2) *Certification.* [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]
- ☐ (i) *The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.*
- ☐ (ii) *The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.*
- (j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly-
- (1) ☐ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or
- (2) ☐ Outside the United States.
- (k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]
- ☐ (1) *Maintenance, calibration, or repair of certain equipment as described in FAR [22.1003-4\(c\)\(1\)](#).* The offeror ☐ does ☐ does not certify that-
- (i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of

- an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;
- (ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR [22.1003-4\(c\)\(2\)\(ii\)](#)) for the maintenance, calibration, or repair of such equipment; and
 - (iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.
- ☐ (2) *Certain services as described in FAR [22.1003-4\(d\)\(1\)](#).* The offeror ☐ does ☐ does not certify that-
- (i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;
 - (ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR [22.1003-4\(d\)\(2\)\(iii\)](#));
 - (iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and
 - (iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.
- (3) If paragraph (k)(1) or (k)(2) of this clause applies—
- (i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and
 - (ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.
- (1) *Taxpayer Identification Number (TIN)* ([26 U.S.C. 6109](#), [31 U.S.C. 7701](#)). (Not applicable if the offeror is required to provide this information to the SAM to be eligible for award.)
- (1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of [31 U.S.C. 7701\(c\)](#) and [3325\(d\)](#), reporting requirements of [26 U.S.C. 6041](#), [6041A](#), and [6050M](#), and implementing regulations issued by the Internal Revenue Service (IRS).
- (2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government ([31 U.S.C. 7701\(c\)\(3\)](#)). If the resulting contract is subject to the payment reporting requirements described in FAR [4.904](#), the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.
- (3) *Taxpayer Identification Number (TIN)*.
- ☐ TIN: _____.
- ☐ TIN has been applied for.
- ☐ TIN is not required because:

☐ Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐ Offeror is an agency or instrumentality of a foreign government;

☐ Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization.*

☐ Sole proprietorship;

☐ Partnership;

☐ Corporate entity (not tax-exempt);

☐ Corporate entity (tax-exempt);

☐ Government entity (Federal, State, or local);

☐ Foreign government;

☐ International organization per 26 CFR 1.6049-4;

☐ Other _____.

(5) *Common parent.*

☐ Offeror is not owned or controlled by a common parent;

☐ Name and TIN of common parent:

Name _____.

TIN _____.

(m) *Restricted business operations in Sudan.* By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) Prohibition on Contracting with Inverted Domestic Corporations.

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at [9.108-2\(b\)](#) applies or the requirement is waived in accordance with the procedures at [9.108-4](#).

(2) *Representation.* The Offeror represents that—

(i) It ☐ is, ☐ is not an inverted domestic corporation; and

(ii) It ☐ is, ☐ is not a subsidiary of an inverted domestic corporation.

(o) Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.

(1) The offeror shall e-mail questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) *Representation and Certifications.* Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

- (iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds the threshold at FAR [25.703-2\(a\)\(2\)](#) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>).
- (3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if-
 - (i) This solicitation includes a trade agreements certification (e.g., [52.212-3\(g\)](#) or a comparable agency provision); and
 - (ii) The offeror has certified that all the offered products to be supplied are designated country end products.
- (p) *Ownership or Control of Offeror.* (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).
 - (1) The Offeror represents that it ☐ has or ☐ does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.
 - (2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:
 Immediate owner CAGE code: _____.
 Immediate owner legal name: _____.
 (Do not use a "doing business as" name)
 Is the immediate owner owned or controlled by another entity: ☐ Yes or ☐ No.
 - (3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:
 Highest-level owner CAGE code: _____.
 Highest-level owner legal name: _____.
 (Do not use a "doing business as" name)
- (q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*
 - (1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that-
 - (i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or
 - (ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has

considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that—

- (i) It is ☐ is not ☐ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and
- (ii) It is ☐ is not ☐ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) *Predecessor of Offeror*. (Applies in all solicitations that include the provision at [52.204-16](#), Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it ☐ is or ☐ is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: (or mark "Unknown").

Predecessor legal name:_____.

(Do not use a "doing business as" name).

(s) [Reserved].

(t) *Public Disclosure of Greenhouse Gas Emissions and Reduction Goals*. Applies in all solicitations that require offerors to register in SAM ([12.301](#)(d)(1)).

(1) This representation shall be completed if the Offeror received \$7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than \$7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)].

(i) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible website the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible website a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible website includes the Offeror's own website or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked "does" in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible website(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

(u)

(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government

agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) *Representation.* By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (*e.g.*, agency Office of the Inspector General).

(v) *Covered Telecommunications Equipment or Services-Representation.* Section 889(a)(1)(A) and section 889 (a)(1)(B) of Public Law 115-232.

(1) The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(2) The Offeror represents that—

(i) It ☐ does, ☐ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(ii) After conducting a reasonable inquiry for purposes of this representation, that it ☐ does, ☐ does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of Provision)

K.3 FAR 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

(b) The use in this solicitation of any Health and Human Services Acquisition Regulations (48 CFR Chapter 3) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

SECTION L - Instructions, Conditions, and Notices to Offerors or Respondents

L.0 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):

<http://www.acquisition.gov/far/> and <https://www.acquisition.gov/hhsar>

HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) PROVISIONS

HHSAR 352.239-73 Electronic and Information Technology Accessibility Notice
(December 2015)

L.1 FULL TEXT FAR PROVISIONS

L.1.1 FAR 52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (NOV 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

(b) The use in this solicitation of any Health and Human Services Acquisition Regulations (48 CFR Chapter 3) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

L.2 FULL TEXT HHSAR PROVISIONS

L.2.1 HHSAR 352.239-72 Information Technology Security Plan and Accreditation (FEB 2024) (Deviation)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in HHSAR 352.239-71 (Deviation), Security Requirements for Information Technology Resources.

(End of provision)

L.2.2 HHSAR 352.239-78 Information and Communication Technology Accessibility Notice (FEB 2024) (DEVIATION)

(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at <https://www.hhs.gov/web/section-508/index.html>. The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see <https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see <https://www.itic.org/policy/accessibility/vpat>), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available at <https://Section508.gov/>.

In order to facilitate the Government's determination whether proposed ICT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility

standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at <http://508.hhs.gov/>. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

L.3 TYPE OF CONTRACT

The Government contemplates award of firm-fixed price contract resulting from this solicitation.

L.4 SERVICE OF PROTEST

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from the Contracting Officer at the email address specified in Section G of the solicitation.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

L.5 NOTICE OF SET-ASIDE

This solicitation is a total set aside for small business concerns.

L.6 FUNDING

There is not currently funding committed for this contract. We do expect that funding will be available; however, a contract will not be awarded until and unless funds become available.

L.7 INQUIRIES/SUBMISSION

All questions/inquiries concerning the solicitation document must be submitted by e-mail (no faxes or telephone calls please) to the Contract Specialist, no later than August 2, 2024 at 12:00 pm Eastern Time. Questions should be e-mailed to the following address:
Jacob.Matthews@psc.hhs.gov

The Government's response to the inquiries will be posted on SAM.gov Contract Opportunities. Any resulting additions, deletions or changes to the solicitation will be made by issuance of a formal amendment. Offerors are instructed specifically to contact only the issuing contract office in connection with any aspect of this requirement prior to contract award. The Government does

not intend to extend the due date for proposals.

The proposal must be submitted no later than August 15, 2024 at 12:00 pm Eastern Time. The Offeror shall submit the proposal to the Contract Specialist at the following email address: Jacob.Matthews@psc.hhs.gov

L.8 GENERAL INSTRUCTIONS

The following instructions establish the acceptable minimum requirements for the format and content of your proposal. The Contracting Officer is the only individual authorized to legally commit the Government to the expenditure of public funds in connection with this requirement. By submitting a proposal in response to this solicitation, it is understood that your proposal shall become a part of the official contract file.

Your attention is directed to the requirements for the submission of technical proposals, business proposals, and past performance information contained in Sections L.9, L.10, and L.11, of the solicitation. Your proposal must be submitted in accordance with these instructions.

The proposal must be prepared in three parts: a "Technical Proposal", a "Business Proposal" and "Past Performance Information." Each of these parts shall be separate and complete in itself so that the evaluation of one may be accomplished independently of the evaluation of the others.

L.9 TECHNICAL PROPOSAL INSTRUCTIONS

Technical proposals shall be limited to 150 double-spaced pages, with 1-inch margins, and using not less than 12 point font. Offerors are encouraged to be succinct and economical in their presentation. Excessive volume and elaborate presentation are unnecessary. Tables of contents, and works cited and the Technical Appendices are not included in the page count.

The technical proposal must not contain references to cost; however, resource information, such as data concerning labor hours and categories, materials, subcontracts, etc., must be contained in the technical proposal so that your understanding of the scope of work may be evaluated. It must disclose your technical approach in sufficient detail to provide a clear and concise presentation that includes, but is not limited to, the requirements of the technical proposal instructions. The proposal shall contain a response to each of the factors and subfactors identified in Section L and will be evaluated in accordance with Section M. Proposals which merely offer to conduct a project in accordance with the requirements of the Government's scope of work will not be eligible for award. The technical proposal should reflect a clear understanding of the nature of the work being undertaken.

Technical Appendices:

The technical appendices shall only include transcripts, resumes, and letters of commitment.

The technical proposal shall address the following factors:

L.9.1 FACTOR 1 - Technical Approach/Understanding of the Requirement

L.9.2 FACTOR 2 – Capability and Experience of the Organization and Proposed Personnel/Management Approach

L.9.3 FACTOR 3 - Information Technology Security Plan and Accreditation Approach

In accordance HHSAR provision 352.239-72 all offers submitted in response to this request for proposal shall address the approach for completing the security plan and accreditation requirements in HHSAR 352.239-71 (Deviation), Security Requirements for Information Technology Resources.

L.9.4 FACTOR 4 - Information and Communication Technology Accessibility

The offeror shall provide the information and documentation required by HHSAR 352.239-78.

L.9.5 OTHER REQUIRED INFORMATION

Offerors shall propose a Quality Assurance Surveillance Plan (QASP) as part of their technical proposal.

L.10 BUSINESS PROPOSAL INSTRUCTIONS (Fixed Price)

The Business Proposal shall contain the following information:

L.10.1 Offerors must complete and include Standard Form 1449. Completion of this form indicates that the Offeror agrees with all the terms and conditions contained in solicitation Sections A through M. In addition, the proposal must contain a statement to the effect that it is firm for a period of at least 120 days from the date of receipt thereof by the Government.

L.10.2 Offerors shall include a completed copy of Section B of the solicitation in its proposal. Business proposals shall include pricing for each contract line item (CLIN) specified in Section B, as well as the total price for the entire contract.

L.10.3 Cost or Pricing Data

- (a) Submission of certified cost or pricing data is not required.
- (b) Provide the data described below:

The Offeror shall submit a price proposal adequate to determine whether the proposed pricing is consistent with the technical proposal.

Data required:

1. Financial Capacity - The Offeror shall indicate if it has the necessary financial capacity, working capital, and other resources to perform this contract without assistance from any outside sources. (If not, indicate the amount required, the anticipated source, and associated costs for such support.) The Offeror shall submit any information deemed relevant to convincingly demonstrate its ability to perform the requirement from a financial point of view; this may include providing a copy of the Offeror's most recent financial statement.

2. Commitments - The Offeror shall list commitments of key personnel with other clients/contracts and indicate whether these commitments will or will not interfere with the completion of work and services contemplated to be completed under this contract.

3. A proposed payment schedule for the contract should be included. The payment schedule should be commensurate with the work to be performed for the contract deliverables and advance payments will not be made.

L.10.4 DISCLOSURE OF LOBBYING ACTIVITIES

Standard Form LLL, "Disclosure of Lobbying Activities" can be accessed in the GSA Forms Library at: <http://www.gsa.gov/portal/forms/download/116430>

L.10.5 REPRESENTATIONS AND CERTIFICATIONS

A completed and executed copy of Section K - Representations, Certifications and Other Statements of Offerors or Respondents, must be included as part of your business proposal.

L.10.6 ORGANIZATIONAL CONFLICT OF INTEREST DISCLOSURE/MITIGATION

Offerors are required to identify actual and potential organizational conflicts of interest (OCI) related to the services described in the statement of work for itself, as well as employees, consultants and subcontractors proposed. This includes, but is not limited to:

- The existence of conflicting roles that might bias judgment; and
- Access to nonpublic information that will give the offeror an unfair competitive advantage.

Offerors shall include an explanation of the process used to identify OCIs. If an actual or potential OCI is identified, the offeror shall submit a mitigation plan as part of its proposal. Offerors shall submit with their proposal an OCI affirmation, using the following language:

"I, (Name and Title), warrant that: 1) I am an official authorized to bind the entity; and 2) to the best of my knowledge and belief, actual and potential organizational conflicts of interest have been identified, and disclosed to the Contracting Officer (identify section of proposal) as of (Date)."

L.10.7 INVOICE PROCESSING PLATFORM WAIVER REQUEST

Offerors may request a waiver from using the Department of Treasury Invoice Processing Platform (IPP) for payment requests, which may be approved by the Contracting Officer for a specific situation, as follows:

- As specified in OMB Memorandum M-15-19, electronic invoicing is not appropriate for the Federal procurement: of relocation services, utilities, or for vendors using PII for identification
- Contractor is in the process of transitioning to electronic submission of payment requests but needs time to complete such transition. Contractor must indicate timeline for transition.
- Contractor demonstrates that electronic submission is unduly burdensome. Contractor must provide full explanation to include substantiating documents when necessary.

IPP waiver requests and supporting documentation shall be included in the business proposal.

L.11 PAST PERFORMANCE INFORMATION INSTRUCTIONS

Offerors will be evaluated on performance under existing contracts and performance on prior contracts. Offerors should note the difference between past performance and past experience. Past performance relates to quality and how well a contractor performed, while past experience is about the type and amount of work previously performed by a contractor.

Past performance information is available to Federal agencies through the Contractor Performance Assessment Reporting System (CPARS). The government will be considering past performance information contained in CPARS to the greatest extent possible.

A maximum of 3 performance references shall be submitted for contracts under which performance has occurred within the past three years. Past performance references can be for the offeror, predecessor companies, key personnel who have relevant experience and/or subcontractors that will perform major or critical aspects of the requirement when such information is relevant to the acquisition.

Each performance reference is limited to 5 pages and shall include the following information:

- Several points of contact (Contracting Officer, Contracting Officer's Representative and any other pertinent officials that can verify performance) - name, agency/company, address, phone number and email address
- For contracts with the Federal Government, indicate whether the government has evaluated the contractor and past performance information is available through CPARS or whether the reference will be providing information via the past performance questionnaire (see Attachment J.1)
- Contract title
- Contract number (and task order number when applicable)
- Contract type
- Total contract value (including base & all options)

- Project description and size information
- If the past performance reference is for a subcontractor, identify the major or critical aspects of the requirement that they will perform
- Relevancy to the statement of work for the subject solicitation
- Did the contract include small business subcontract goals for small disadvantaged business concerns? If so, were the goals met?
- Provide an explanation of problems, delays, cost overruns and corrective actions taken.

In addition to the past performance information specified above:

For contracts that have performance information available through CPARS, offerors are requested to provide a copy of the CPARS report.

For contracts that do not have performance information available through CPARS, offerors are requested to provide the Past Performance Questionnaire (Attachment J.1) directly to their reference. The reference should complete the questionnaire and submit information directly back to the Government via email to Jacob.matthews@psc.hhs.gov by the close date of this solicitation.

Past performance information is proprietary source selection information. The Government will only discuss past performance information directly with the entity or person that is being reviewed. If there is a problem with the proposed subcontractor's past performance, the prime can be notified of a problem, but no details may be discussed without the subcontractor's permission.

SECTION M - Evaluation Factors for Award

M.1 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):

<http://www.acquisition.gov/far/>

FAR 52.217-5 EVALUATION OF OPTIONS

M.2 GENERAL

The Contracting Officer may eliminate from the competition any proposal that was not submitted in accordance with the solicitation instructions.

M.3 AWARD WITHOUT DISCUSSIONS AND COMPETITIVE RANGE DETERMINATIONS

The Government intends to evaluate proposals and award a contract without discussions with Offerors (except for clarifications as described in FAR 15.306(a)). Therefore, the Offeror's initial proposal should contain the Offeror's best terms from a cost or price and technical standpoint. The Government reserves the right to conduct discussions if the Contracting Officer later determines them to be necessary. In the event discussions are held, a competitive range determination will be made. If the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals.

M.4 BASIS FOR AWARD

The following factors will be considered in evaluating proposals, in descending level of importance:

- Technical (sub-factors are numbered in descending level of importance);
 - Technical Approach/Understanding of the Requirement
 - Capability and Experience of the Organization and Proposed Personnel/Management Approach
 - Information Technology Security Plan and Accreditation Approach
 - Information and Communication Technology Accessibility

- Price;
- Past Performance

Award will be made to that responsible Offeror whose proposal contains the combination of those factors offering the best overall value to the Government utilizing the tradeoff process. This will be determined by comparing differences in technical merit and past performance with differences in cost to the Government. The Government reserves the right to make an award to other than the lowest priced offeror or to the offeror with a higher technical score if the Contracting Officer determines that to do so would result in the best value to the Government. All evaluation factors other than price, when combined, are significantly more important than price. The following table reflects the relative order of importance regarding the “technical”

M.5 (ALTERNATE) TECHNICAL EVALUATION CRITERIA – COLOR/ADJECTIVAL METHOD

The Government will evaluate the Technical Proposal using the following color/adjectival coded ratings. Each factor will receive one of the color/adjectival coded ratings defined below, and then there will be an overall color/adjectival coded rating for the proposal.

Color/Adjective	Definitions
Blue/Outstanding	Significantly exceeds most or all solicitation requirements for this factor or subfactor OR otherwise demonstrates a very high probability of successful contract performance. Response exceeds a “Green/Excellent” rating.
Green/Excellent	Fully meets all solicitation minimum requirements and exceeds many of the solicitation requirements for this factor or subfactor or overall; OR exceeds a small number of the minimum requirements but to a significant degree or in a valuable way for this factor or subfactor or overall; OR otherwise demonstrates a high probability of successful contract performance. Response exceeds a “Yellow/Acceptable” rating.
Yellow/Acceptable	Fully meets all solicitation minimum requirements for this factor or subfactor or overall OR otherwise demonstrates an average probability of successful contract performance. Areas where the proposal exceeds the minimum solicitation requirements, if any, are of little or no value to the Government.
Orange/Marginal	Less than “Yellow/Acceptable.” Does not meet all solicitation minimum requirements for this factor or subfactor or overall OR otherwise demonstrates a moderate risk of unsuccessful contract performance. The proposal indicates a superficial or vague understanding of the program goals and the methods, resources, schedules and/or other aspects essential to contract performance.
Red/Unacceptable	Technical proposal has one (or more) deficiency and/or substantial omissions for a factor or subfactor or overall AND/OR the proposal demonstrates a lack of understanding of the program goals, methods, resources, schedules and/or other aspects essential to contract performance. The risk of unsuccessful contract performance is high.

The criteria identified below will serve as the standard against which the technical proposal will be evaluated and identifies the significant factors which the Offeror should address in their proposal. The criteria will be used to technically evaluate proposals and are listed in descending order of importance with Factor 1 being most important:

M.5.1 FACTOR 1 - Technical Approach/Understanding of the Requirement

The technical proposal should reflect a clear understanding of the nature of the work being undertaken, analyzed, staffed, and managed, as well as the Offeror’s overall understanding of the mission of the Program Office and the specific culture of this requirement. The proposal must

outline a clear understanding of the primary requirement – that the system must be operational to provide uninterrupted payroll services no later than 1 January 2025. The Offeror demonstrates understanding of the work to be performed, the ability to perform the work under the contract in a timely manner and the complex issues surrounding the tasks and services required for the operations and maintenance of existing IT data and payroll and personnel processing functions including but not limited to IT pay generation, disbursement, and officer personnel system. The Offeror shall ensure that its proposal identifies how its capabilities map to the overall needs of the requirements outlined within the PWS. The technical proposal should provide a detailed technical description and overall project work plan for achieving the project objectives and all the required tasks indicated in the PWS. The plan should address how specific tasks in the PWS will be accomplished, as well as how the tasks are related. The plan should include milestones and/or phasing charts to illustrate a logical sequence of proposed events. The proposal should reflect an outstanding plan to conduct the project with an approach that is clear, complete, reasonable, and feasible. Technical proposals should reflect Offerors' experience with similar projects and describe how past efforts and strategies have resulted in effective execution of similar projects and/or the use of techniques similar to those proposed here as well as how they intend to ensure continued innovative and evolving high quality service offerings over time. Offerors are expected to provide a technical approach that is innovative, relevant to the current policy and programmatic environment, of the highest scientific quality and rigor, and consistent with effective project management. The approach to each task should be the most appropriate to achieve the objectives and produce high-quality deliverables within the constraints of resources and schedule utilizing realistic timeframes and identifying the chronological sequence by which key activities will occur in order to ensure the completion of each task that the Contractor will be responsible for performing.

Risk Management- Methodology for identifying, tracking, and reporting risks associated with its proposed IT solution. This includes the Offeror's method for mitigating threats and capturing opportunities presented by the identified risks. The Offeror shall identify the key risks associated with their proposed solution and the proposed response to those risks.

Transition Tasks and Management - Provide a detailed draft Transition Plan that describes how you will transition-in all services to be provided under this contract during the 60-day Transition-In period post award. The draft Transition Plan shall detail all specific actions and critical steps that need to be taken and their expected completion dates with task dependencies for transitioning-in each existing IT, personnel, and payroll process and/or function and all PWS requirements required to assume 100% ownership of all IT, Personnel and Payroll Function by January 1, 2025. The transition plan shall elaborate on managing transition issues and risks to ensure minimal disruption. The draft Transition Plan should also describe your approach to transitioning-out of activities, to include documentation, knowledge transfer, user manuals, how-to guides training, and support to CCHQ to ensure a successful transition to another contractor, e.g., describe how you will ensure that corporate best-in-class approaches to Program Management and Project Management are being disseminated to the project teams throughout transition and continuing through the contract duration. Discussion of the transition and migration process to move the existing IT data to the vendor's integrated personnel and payroll solution. Discussion of the transition and migration of the existing IT data to the vendor's integrated personnel and payroll solution to include but not limited to learning curves, technical

knowledge transfers, on-boarding, etc. Discussion of the contractor's ability to meet PWS section 2.3 Conditions for Transition Completion and PWS section 3.8 Conditions for Successful System Handover by January 1, 2025, to ensure uninterrupted payroll and personnel services and/or processes ensuring continuity of operations.

M.5.2 FACTOR 2 - Capability and Experience of the Organization and Proposed Personnel/Management Approach

CAPABILITY AND EXPERIENCE OF THE ORGANIZATION AND PROPOSED PERSONNEL The proposal should demonstrate a proven organizational track record in executing the tasks described in the O&M tasks within the PWS; the organization's history of successful completion of projects similar in scope, meeting deadlines and demonstrating flexibility in addressing changes in schedules; and providing overall customer satisfaction. For any subcontractors or consultants proposed, clearly document their roles and responsibilities, describe their added value to the project, and demonstrates that they have previous organizational experience in performing work similar to that outlined in the PWS. Provide detailed information regarding the personnel who would be assigned to the project (including any proposed consultants and subcontractors). Include a description of the proposed roles and major responsibilities of proposed staff (i.e., principal investigators, project directors, senior advisors, project managers, and task leaders). The proposal should demonstrate that the personnel have the technical qualifications and academic, professional, and technical experience to complete the functions and duties they would perform. The Offeror must include a list of names, positions/titles and proposed duties of all proposed professional personnel, consultants, and key subcontractor employees assigned to the project to include but not limited to the following identified key positions: Project Manager, Software Developers/Programmers Software Architect, UI/UX Software Designer, Quality Assurance Specialist, SCRUM Master, Business Analyst, IT Security Specialist, Database Administrator/Programmer, and Help Desk Support. Their resumes should be included and should contain information on education, background, recent experience, and specific technical accomplishments. Resumes and letters of commitment for proposed personnel must be included in the Technical Appendix.

Staffing Approach- Propose a staffing plan that describes who you plan to use and how their prior experiences on similar tasks align with their roles and responsibilities in the technical approach. Describe how you will acquire and retain qualified and experienced personnel throughout the life of the contract. This approach must include how you attract, motivate, and retain a qualified workforce. Include your approach and process for replacement of personnel. Describe how you train your workforce and, specifically, how you ensure personnel proficiencies are maintained and that your workforce stays current with technology changes, innovative approaches, and trending methodologies throughout the life of the contract. The staffing plan must identify subcontractor(s), if any, who will be used under the task orders and their qualifications. Provide proposed staffing, labor category, roles and description, number of FTEs and number of hours.

Provide résumés for the Key Personnel Proposed- Resumes should clearly demonstrate the degree of experience as it relates to the requirements of the PWS. Qualifications of the proposed key personnel regarding the education and professional certifications/credentials. The resume

must include:

- Employment history, including employer's name, position title, duties and responsibilities and dates/time frame;
- Applicable skills, experience expertise and qualifications; and
- Relevant education, credentials and or certifications including dates.
- Qualifications of the proposed key personnel regarding the experience in similar projects (e.g., size, scope, magnitude, duration, and complexity etc.)

MANAGEMENT APPROACH- The Offeror must provide information which will demonstrate an understanding of how to manage the stated tasks. The Offeror must explain how the management and coordination of contractor staff and/or subcontractor efforts will be accomplished. This must include an organization/staff loading chart depicting the contracting and subcontracting staff structure supporting the project. The labor categories and approximate percentage of time that each individual will be available for this project must be included to allow the Government to consider whether the level of effort and labor mix are appropriate for the work to be performed. The proposed staff hours for each of the above individuals should be allocated against each task or subtask for the project. Management plans must be sound, feasible, and show clear lines of authority and responsibility with quality control procedures. The Offeror must also submit a Quality Control Plan that will be used to ensure high-quality performance that meet the requirements and expectations indicated in the PWS. This includes, but is not limited to, procedures for reporting progress, foreseeing potential problems and/or risks and providing a plan to mitigate those problems/risks, and ensuring effective communication among the entities involved, as well as the Contracting Officer's Representative and the Contracting Officer. The Offeror's Management plan will be evaluated on how well it demonstrates that assigned contractor personnel will have the ability to meet contract deliverables, resolve issues in a timely manner, and successfully complete the requirements on schedule, within budget and within acceptable quality levels.

Quality Control- Discuss the degree to which your approach meets or exceeds our quality control expectations as specified in the solicitation, including the quality assurance approach and plan to adequately meet all deliverables. The management plan includes procedures for reporting progress, foreseeing potential problems and/or risks and providing a plan to mitigate those problems/risks, and ensuring effective communication among the entities involved, as well as the Contracting Officer's Representative and the Contracting Officer. Discuss your communication and internal controls that will ensure achievement of all requirements including adherence to contract clauses and compliance with the overall contract. Discuss your approach to sharing performance and progress against all tasks/requirements in accordance with the PWS. Discuss the management tools with sufficient detail and/or graphical depiction that you would utilize to give CCHQ real-time access and visibility to monitor and track contract deliverables, schedule, cost, and performance. How the contractor will identify and escalate critical issues and information as well as an explanation of the controls and people that are involved in the decision-making process. Explanation of the Offeror's proposed method of communicating this information to DHS stakeholders at all levels.

Information Technology Solutions Life Cycle Management (ITSLCM) Framework - Details the Offeror's approach to managing CCHQ's requirements through the ITSLCM framework.

M.5.3 FACTOR 3 - Information Technology Security Plan and Accreditation Approach

The approach to completing the security plan and accreditation requirements in accordance with HHSAR 352.239-71 (Deviation) will be evaluated for suitability.

M.5.4 FACTOR 4 - Information and Communication Technology Accessibility

The completed HHS Section 508 Accessibility Conformance Checklist (see <https://www.hhs.gov/web/section-508/accessibility-checklists/index.html>) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see <https://www.itic.org/policy/accessibility/vpat>) will be assessed as to whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards. If ICT does not conform and cannot be acceptably remediated, rationale for the perceived exemption or exception must be provided. Potential exemptions and exceptions are identified in FAR subparts [39.204](#) and [39.205](#). The government determines whether an exemption or exception can be appropriately applied.

M.5.4 Factor 4, Information and Communication Technology Accessibility evaluation criterion will be evaluated as Acceptable or Unacceptable.

Section 508 Compliance rating:

Rating	Symbol	Description
Acceptable	A	The proposal meets the stated requirements. The proposal includes a completed HHS 508 Evaluation that demonstrates compliance with the established EIT accessibility standards and a binding statement of conformance to the established EIT accessibility standards.
Unacceptable	U	The proposal fails to meet the stated requirements. The proposal does not include a completed HHS 508 Evaluation that demonstrates compliance with the established EIT accessibility standards and a binding statement of conformance to the established EIT accessibility standards.

M.6 PAST PERFORMANCE EVALUATION

Past performance information is one indicator of an offeror's ability to perform the contract successfully. This evaluation is subjective and will be based on information obtained from references provided by the offeror, as well as information obtained by other sources known to the Government. For the purpose of this evaluation the term "offeror" is inclusive of the prime, predecessor companies, key personnel and subcontractors for which past performance will be evaluated.

The Government will consider the relevancy and quality of the offeror's past performance to

assess the risk of unsuccessful contract performance. If quality information is not available for a reference, the reference will not be evaluated for relevancy, nor considered in determining the overall risk rating.

STEP 1 - Relevancy

Each reference will be evaluated for relevancy based on the scope and magnitude of effort and complexities of the work performed and how it compares to the services specified in Section C of this solicitation.

Rating	Definition
Very Relevant	Performance effort involved essentially the same scope and magnitude of effort and complexities this solicitation requires.
Relevant	Performance effort involved similar scope and magnitude of effort and complexities this solicitation requires.
Somewhat Relevant	Performance effort involved some of the scope and magnitude of effort and complexities this solicitation requires.
Not Relevant	Performance effort involved little or none of the scope and magnitude of effort and complexities this solicitation requires.

STEP 2 - Quality

To determine how well the offeror has performed in the past, the Government is using past performance rating information available in CPARS, information provided by references, as well as information obtained by other sources known to the Government.

Each reference will be evaluated for the overall quality of the performance.

Rating	Definition
Excellent	The contractor has performed successfully and greatly exceeded expectations under the contract.
Good	The contractor has performed successfully and exceeded expectations under the contract.
Acceptable	The contractor has performed successfully under the contract.
None	No record of performance or performance is inconclusive

Mediocre	The contractor has some unsuccessful performance under the contract.
Deficient	The contractor has performed unsuccessfully under the contract.

STEP 3 - Risk Rating

After considering the relevancy and the quality of the offerors past performance, an overall risk rating will be determined for each offeror. The risk rating is an assessment of the overall risk of unsuccessful contract performance based on the past performance of the offeror. The more relevant the references are to the current acquisition, the more significant the reference becomes and the more weight it is given in determining the risk rating. Adverse past performance information on references that are not deemed to be relevant may be taken into consideration in determining the risk rating if the adverse information is considered to have bearing on the current acquisition. The Government will consider the type and amount of work to be performed by the prime, key personnel, and major or critical subcontractors to determine the significance of their past performance information when determining the risk rating. In the case of an offeror without a record of relevant past performance or for whom information on past performance is not available or is inconclusive, the offeror will not be evaluated favorably or unfavorably on past performance.

Rating	Description
Unknown Performance Risk	No performance record is identifiable, past performance is not relevant to the required effort, or the past performance information is inconclusive
Very Low Performance Risk	Based on the offeror's performance record, no doubt exists that the offeror will successfully perform the required effort
Low Performance Risk	Based on the offeror's performance record, minimal doubt exists that the offeror will successfully perform the required effort.
Moderate Performance Risk	Based on the offeror's performance record indicating some unsuccessful contract performance, some doubt exists that the offeror will successfully perform the required effort.
High Performance Risk	Based on the offeror's performance record indicating unsuccessful contract performance, substantial doubt exists that the offeror will successfully perform the required effort.

M.7 (ALTERNATE 1) PRICE EVALUATION (Fixed Price)

The price proposal will be evaluated for reasonableness. For a price to be reasonable, it must represent a price to the government that a prudent person would pay when consideration is given to prices in the market. Normally, price reasonableness is established through adequate price competition, but may also be determined through cost and price analysis techniques as described in FAR 15.404.

M.8 RESPONSIBILITY

To be eligible for award, an Offeror must be determined responsible in accordance with the standards in FAR Part 9.104.

M.9 ORGANIZATIONAL CONFLICT OF INTEREST

If the Government determines that an organizational conflict of interest (OCI) exists, that cannot be satisfactorily avoided, neutralized or mitigated or waived, the Contracting Officer may determine that the offeror will not be eligible for award. The Government reserves the right to only consider mitigation plans proposed by the apparent successful offeror. If this acquisition is governed by FAR Part 15, the process of approving an OCI mitigation plan and revisions to such a plan does not constitute discussions as described in FAR 15.306.