

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30</i>				1. REQUISITION NUMBER		PAGE OF 1 78		
2. CONTRACT NO.		3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER		5. SOLICITATION NUMBER		6. SOLICITATION ISSUE DATE	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME HEIDI HOLLEY			b. TELEPHONE NUMBER (No collect calls) +1 301 496 0612		8. OFFER DUE DATE/LOCAL TIME	
9. ISSUED BY National Institutes of Health Office of Logistics and Office of Administration 6011 Executive Blvd Rockville, MD 20852-3804				CODE OD/OLAO-OA	10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A) NAICS: 541990 SIZE STANDARD: \$16.5			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input checked="" type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		<input type="checkbox"/> 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b. RATING		
15. DELIVER TO 6700B, RCKLDGE, BTHOFF Rockledge 6700 6700B Rockledge Dr Bethesda, MD 20817		CODE 6700B, RCKLDGE, BTHOFF	16. ADMINISTERED BY National Institutes of Health OD - Office of Logistics and Acquisition Operations Bethesda, MD 20892-7511					CODE OD/OLAO
17a. CONTRACTOR/ OFFEROR		CODE L6R3M86AFBB5	FACILITY CODE	18a. PAYMENT WILL BE MADE BY 2115 E Jefferson St MSC 8500 Suite 4B 432 Bethesda, MD 20892-8500				CODE 2115 E JEFFERSON
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	
	This IDIQ contract is for the National Institutes of Health (NIH) Business and Professional Support Services that covers a wide range of services including Analysis, Business Solutions, and Acquisition Lifecycle Support; Business Process Improvement and Organizational Assessment; Communication and Training; Program Planning and Management Services; Policy Development, Implementation, and Administration; System Integration; and Centers of Excellence Support Services. <i>(Use Reverse and/or Attach Additional Sheets as Necessary)</i>							
25. ACCOUNTING AND APPROPRIATION DATA See schedule						26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$49,000,000.00		
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE 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.				
<input type="checkbox"/> 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.				
<input type="checkbox"/> 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.					<input type="checkbox"/> 29. AWARD OF CONTRACT: _____ 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)		31c. DATE SIGNED		
				TERITA R. STEVENSON				

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
1	<p>The contractor, acting as an independent contractor and not as an agent of the government, shall furnish all materials, personnel, facilities, support, and management necessary to meet the requirements of task orders issued under this IDIQ and in accordance with the Statement of Work. The contract type is an Indefinite Delivery/Indefinite Quantity (IDIQ) task order contract utilizing Fixed Price(FP), Labor Hour, and Time and Materials (T&M) type task orders in accordance with FAR 16.504. This contract will be used primarily by NIH, but may also be used by other portions of DHHS and other Federal agencies. Base period: August 13, 2022 to August 12, 2023 Option 1: August 13, 2023 to August 12, 2024</p> <p>POCs: COR: Jeff Klein, jeff.klein@nih.org Contract Specialist: Heidi Holley, heidi.holley@nih.org Contractor: Delivery: 08/12/2024 Period of Performance: 08/13/2022 to 08/12/2024</p> <p>NIH Business and Professional Support Services (BPSS) III Obligated Amount: \$0.00 Continued ...</p>				49,000,000.00

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 <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	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
--	--------------------	---------------------------------	--	------------------

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	41c. DATE	42b. RECEIVED AT (<i>Location</i>)
		42c. DATE REC'D (YY/MM/DD)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

PAGE OF

3

78

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: R499 Product/Service Description: SUPPORT- PROFESSIONAL: OTHER				

TABLE OF CONTENTS

PART I - THE SCHEDULE 2
 SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS..... 2
 SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT 4
 SECTION D - PACKAGING, MARKING AND SHIPPING 10
 SECTION E - INSPECTION AND ACCEPTANCE 11
 SECTION F - DELIVERIES OR PERFORMANCE 12
 SECTION G - CONTRACT ADMINISTRATION DATA 13
 SECTION H - SPECIAL CONTRACT REQUIREMENTS 20
PART II - CONTRACT CLAUSES 46

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS 57
 SECTION J - LIST OF ATTACHMENTS 57

PART IV - REPRESENTATIONS AND INSTRUCTIONS 57
 SECTION K - REPRESENTATIONS AND CERTIFICATIONS 57

PART I - THE SCHEDULE

THE INFORMATION SET FORTH IN **SECTION A - SOLICITATION/CONTRACT FORM**, HEREIN CONTAINS IMPORTANT INFORMATION FOR ANY OFFEROR INTERESTED IN RESPONDING TO THIS SOLICITATION. ANY CONTRACT RESULTING FROM THIS SOLICITATION WILL INCLUDE IN ITS **SECTION A - SOLICITATION/ CONTRACT FORM**, ACCOUNTING, APPROPRIATION AND GENERAL INFORMATION APPLICABLE TO THE CONTRACT AWARD.

THE CONTRACT SCHEDULE SET FORTH IN **SECTIONS B THROUGH H**, HEREIN, CONTAINS CONTRACTUAL INFORMATION PERTINENT TO THIS SOLICITATION. IT IS NOT AN EXACT REPRESENTATION OF THE CONTRACT DOCUMENT THAT WILL BE AWARDED AS A RESULT OF THIS SOLICITATION. THE CONTRACT COST OR PRICE AND OTHER CONTRACTUAL PROVISIONS PERTINENT TO THE OFFEROR (i.e., those relating to the organizational structure [e.g., Non-Profit, Commercial] and specific cost authorizations unique to the Offeror's proposal and requiring Contracting Officer Prior Approval) WILL BE DISCUSSED IN THE NEGOTIATION PROCESS AND WILL BE INCLUDED IN THE RESULTANT CONTRACT. THE ENCLOSED CONTRACT SCHEDULE IS INTENDED TO PROVIDE THE OFFEROR WITH THE NECESSARY INFORMATION TO UNDERSTAND THE TERMS AND CONDITIONS OF THE RESULTANT CONTRACT.

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

ARTICLE B.1. BRIEF DESCRIPTION OF SUPPLIES OR SERVICES

The National Institutes of Health (NIH) intends to acquire a wide range of Business and Professional Support Services for Financial Analysis, Business Solutions, and Acquisition Lifecycle Support; Business Process Improvement and Organizational Assessment; Communication and Training; Program Planning and Management Services; Policy Development, Implementation, and Administration; System Integration; and Centers of Excellence Support Services.

The contractor, acting as an independent contractor and not as an agent of the government, shall furnish all the necessary services, qualified personnel, material, equipment, and facilities necessary to meet the requirements in accordance with the Statement of Work. The contract type is an Indefinite Delivery/Indefinite Quantity (IDIQ) task order contract utilizing Fixed Price(FP), Labor Hour, and Time and Materials (T&M) type task orders in accordance with FAR 16.504. This contract will be used primarily by NIH, but may also be used by other portions of DHHS and other Federal agencies.

ARTICLE B.2. HISTORICAL REFERENCE MATERIALS

This acquisition is the follow-on to the NIH Business and Professional Support Services II (NIHBPSSII) contract. Reference material pertinent to the original contracts is available at <https://nihbpss.olao.od.nih.gov/resources.html>.

ARTICLE B.3. PRICES/COSTS

- a. This is a Multiple Award Indefinite Quantity contract as contemplated by FAR 16.504. The Contractor shall be reimbursed by the Government in an amount not less than a total of \$250 (minimum) nor more than a total of \$49,000,000.00. (maximum) for successful performance of this contract.
- b. The prices set forth in this ARTICLE will cover the contract period August 13, 2022 to August 12, 2024.
- c. The Government will compete and award Task Orders based on the work described in SECTION C of this contract.
- d. Ordering procedures are described in The TASK ORDER PROCEDURE Article in SECTION G of this contract.

- e. The Government shall compensate the Contractor at an amount negotiated at task order award. Compensation will be negotiated on the basis of the Labor Rates set forth below:

Business and Professional Support Services Labor Category	Hourly Rate (fully loaded) Base Year	Hourly Rate (fully loaded) Option Year 1
AA: Project Manager		
AB: Assistant Project Manager		
AC: Administrative Assistant		
AD: Web Project Manager		
AE: Web Designer		
AF: Web Software Developer		
AG: Web Content Administrator		
AH: Budget Analyst		
AI: Accounting Analyst		
AJ: Financial Manager		
AK: Procurement Specialist		
AL: Subject Matter Expert		
AM: Logistical/Technical Support Specialist		
AN: Functional Specialist		
AO: Subject Matter Expert Instructor		
AP: Business Process Reengineering Specialist		
AQ: Software Architect		
AR: Business Operations Specialist		
AS: Human Resources Analyst		

ARTICLE B.4. ADVANCE UNDERSTANDINGS

Specific elements of cost, which normally require prior written approval of the Contracting Officer before incurrence of the cost (e.g., foreign travel, consultant fees, subcontracts) will be included in this Article if the Contracting Officer has granted his/her approval prior to contract award.

SECTION C - DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

ARTICLE C.1. DESCRIPTION -STATEMENT OF WORK

- a. Independently and not as an agent of the Government, the Contractor shall be required to furnish all the necessary services, qualified personnel, material, equipment, and facilities, not otherwise provided by the Government, as needed to perform the Statement of Work attached hereto and made a part of this contract (See SECTION J - List of Attachments).

ARTICLE C.2. REPORTING REQUIREMENTS

The fill-ins for this article will be determined at the task order level.

All reports required herein shall be submitted in electronic format. In addition, one hardcopy of each report shall be submitted to the Contracting Officer.

All electronic reports submitted shall be compliant with Section 508 of the Rehabilitation Act of 1973. Additional information about testing documents for Section 508 compliance, including guidance and specific checklists, by application, can be found at: <http://www.hhs.gov/web/508/index.html> under "Making Files Accessible."

All paper/hardcopy documents/reports submitted under this contract shall be printed or copied, double-sided, on at least 30 percent post consumer fiber paper, whenever practicable, in accordance with FAR 4.302(b).

a. Technical Progress Reports

1. In addition to the required reports set forth elsewhere in this Schedule, the preparation and submission of regularly recurring Technical Progress Reports will be required in any contract resulting from this solicitation. These reports will require descriptive information about the activities undertaken during the reporting period and will require information about planned activities for future reporting periods. The frequency and specific content of these reports will be determined prior to contract award.

For proposal preparation purposes only, it is estimated that in addition to the required electronic version(s) 0 hard copies of these reports will be required as follows:

- Monthly
- Quarterly
- Semi-Annually
- Annually
- Annually (with a requirement for a Draft Annual Report)
- Final - Upon final completion of the contract
- Final - Upon final completion of the contract (with a requirement for a Draft Final Report)

b. Other Reports/Deliverables. na

HHS SECURITY AND PRIVACY LANGUAGE FOR INFORMATION AND IT PROCUREMENTS

INFORMATION AND/OR PHYSICAL SECURITY

- A. **Security Assessment and Authorization (SA&A)**- A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system

under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) within three (3) months after contract award. The Contractor shall conduct the SA&A requirements in accordance with HHS IS2P, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (latest revision).

For an existing ATO, Contracting Officer Representative must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such. NIH acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

- B. **SA&A Package Deliverables** - The Contractor (and/or any subcontractor) shall provide an SA&A package within 30 days of contract award to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package.
- **System Security Plan (SSP)** - due within 30 days after contract award. The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline requirements, and other applicable NIST guidance as well as HHS and NIH policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter.
 - **Security Assessment Plan/Report (SAP/SAR)** - due 30 days after the contract award. The security assessment shall be conducted by the assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and NIH policies. The assessor will document the assessment results in the SAR.

The NIH should determine which security control baseline applies and then make a determination on the appropriateness/necessity of obtaining an independent assessment. Assessments of controls can be performed by contractor, government, or third parties, with third party verification considered the strongest. If independent assessment is required, include statement below.

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

- **Independent Assessment** - due 90 days after the contract award. The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). 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. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).

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

C. **Contingency Plan and Contingency Plan Test** - due 60 days after contract award. 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 NIH policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least annually.

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

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

D. 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:

Level 6: Public Trust - High Risk. Contractor/subcontractor employees assigned to Level 6 positions shall undergo a Suitability Determination and Background Investigation (MBI).

Level 5: Public Trust - Moderate Risk. Contractor/subcontractor employees assigned to Level 5 positions with no previous investigation and approval shall undergo a Suitability Determination and a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI).

Level 1: Non-Sensitive. Contractor/subcontractor employees assigned to Level 1 positions shall undergo a Suitability Determination and National Check and Inquiry Investigation (NACI).

1. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-12

Roster-

- a. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within fourteen (14) calendar days after the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within seven (7) calendar days of the change.

The COR will notify the Contractor of the appropriate level of investigation required for each staff member. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for contractor use at: https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/SuitabilityRoster_10-15-12.xlsx.

- b. If the Contractor is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification.
- c. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification.
- d. The Contractor shall notify the Contracting Officer in advance when any new personnel, who are subject to a background check/investigation, will work under the contract and if they have previously been the subject of national agency checks or background investigations.
- e. All contractor and subcontractor employees shall comply with the conditions established for their designated position sensitivity level prior to performing any work under this contract. Contractors may begin work after the fingerprint check has been completed.
- f. Investigations are expensive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with the FAR clause, Excusable Delays - see FAR 52.249-14. Accordingly, the Contractor shall ensure that any additional employees whose names it submits for work under this contract have a reasonable chance for approval.
- g. Typically, the Government investigates personnel at no cost to the Contractor. However, 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 additional investigation(s).
- h. The Contractor shall include language similar to this "HHS Controlled Facilities and Information Systems Security" language in all subcontracts that require subcontractor personnel to have the same frequency and duration of (1) physical access to an HHS-controlled facility; (2) logical access to an HHS-controlled information system; (3) access to sensitive HHS data/information, whether in an HHS-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3).
- i. The Contractor shall direct inquiries, including requests for forms and assistance, to the Contracting Officer or designee.
- j. Within 7 calendar days after the Government's final acceptance of the work under this contract, or upon termination of the contract, the Contractor shall return all identification badges to the Contracting Officer or designee.

E. CONTRACT INITIATION AND EXPIRATION

1. **General Security Requirements-** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the HHS EPLC framework and methodology or and in accordance with the HHS Contract Closeout Guide (2012). HHS EA requirements may be located here: <https://www.hhs.gov/ocio/ea/documents/proplans.html>
2. **System Documentation-** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

3. **Sanitization of Government Files and Information-** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation in accordance with the NIH Media Sanitization and Disposal Policy to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
 4. **Notification-** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within fifteen days before an employee stops working under this contract.
 5. **Contractor Responsibilities Upon Physical Completion of the Contract-** The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or NIH policies.
 6. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the NIH Contractor Employee Separation Checklist <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Emp-sep-checklist.pdf> when an employee terminates work under this contract within 2 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.
- F. **Contractor Non-Disclosure Agreement (NDA)-** Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the NIH non-disclosure agreement <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf> , as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
- G. **Vulnerability Scanning Reports**
 The Contractor shall report the results of the required monthly special vulnerability scans no later than 10 days following the end of each reporting period. If required monthly, this report may be included as part of the Technical Progress Report. Otherwise, this report shall be submitted under a separate cover on monthly basis.
- H. **Government Access for Security Assessment.** In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:
- a. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.
 The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.
 - b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure

to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

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

2. Section 508 Annual Report

The contractor shall submit an annual Section 508 report in accordance with the schedule set forth by the Contracting Officer (CO)/Contracting Officer's Representative (COR). The Section 508 Report Template and Instructions for completing the report are available at: <http://www.hhs.gov/web/508/contracting/technology/vendors.html> under "Vendor Information and Documents."

SECTION D - PACKAGING, MARKING AND SHIPPING

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

SECTION E - INSPECTION AND ACCEPTANCE

- a. The Contracting Officer or the duly authorized representative will perform inspection and acceptance of materials and services to be provided.
- b. For the purpose of this SECTION, task order contracting officer's representative is the authorized representative of the Contracting Officer.
- c. Inspection and acceptance will be performed at a location specified in the task order

SECTION F - DELIVERIES OR PERFORMANCE

ARTICLE F.1. PERIOD OF PERFORMANCE

- a. The period of performance of this contract shall be from the date of award through 12 months thereafter.
- b. If the Government exercises its option(s) pursuant to the OPTION PROVISION Article in Section H of this contract, the period of performance will be increased as listed below:

Option	Option Period
Base Period	August 13, 2022 - August 12, 2023
Option Year I	August 13, 2023 - August 12, 2024

ARTICLE F.2. CLAUSES INCORPORATED BY REFERENCE, FAR 52.252-2 (FEBRUARY 1998)

This contract incorporates the following clause(s) by reference, with the same force and effect as if it were given in full text. Upon request, the Contracting Officer will make its full text available. Also, the full text of a clause may be accessed electronically at this address: <https://www.acquisition.gov/?q=browsefar>.

FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSE:

52.242-15, Stop Work Order (August 1989)

Alternate I (April 1984) is not applicable to this contract.

SECTION G - CONTRACT ADMINISTRATION DATA

ARTICLE G.1. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The following Contracting Officer's Representative (COR) will represent the Government for the purpose of this contract:

Jeff Klein

The COR is responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and recommending to the Contracting Officer changes in requirements; (2) interpreting the statement of work and any other technical performance requirements; (3) performing technical evaluation as required; (4) performing technical inspections and acceptances required by this contract; and (5) assisting in the resolution of technical problems encountered during performance.

[The alternate COR is responsible for carrying out the duties of the COR only in the event that the COR can no longer perform his/her duties as assigned.]

The Contracting Officer is the only person with authority to act as agent of the Government under this contract. Only the Contracting Officer has authority to: (1) direct or negotiate any changes in the statement of work; (2) modify or extend the period of performance; (3) change the delivery schedule; (4) authorize reimbursement to the Contractor for any costs incurred during the performance of this contract; (5) otherwise change any terms and conditions of this contract; or (6) sign written licensing agreements. Any signed agreement shall be incorporated by reference in Section K of the contract

The Government may unilaterally change its COR designation.

ARTICLE G.2. KEY PERSONNEL, HHSAR 352.237-75 (December 2015)

The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to the contractor voluntarily diverting any of the specified individuals to other programs or contracts the Contractor shall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractor is terminated for cause or separates from the contractor voluntarily with less than thirty days notice, the Contractor shall provide the maximum notice practicable under the circumstances. The Contractor shall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

(End of Clause)

The following individual(s) is/are considered to be essential to the work being performed hereunder:

Name	Title
	Program Manager

ARTICLE G.3. METHOD OF ORDERING

a. Orders issued under this contract may be placed as follows:

in writing

via telephone

via facsimile (fax)

via electronic mail (e-mail)

Oral [Oral Orders will be confirmed in writing within__days of issuance.

Other Specify: _____

- b. The Contracting Officer is authorized to issue orders and provide written confirmation of oral orders, if applicable, under the contract.

ARTICLE G.4. TASK ORDER PROCEDURE

This contract provides for the issuance of Task Orders on a negotiated basis as follows:

a. General

Only the Contracting Officer may issue Task Orders to the Contractor, providing specific authorization or direction to perform work within the scope of the contract and as specified in the Statement of Work. Unless specifically authorized by the Contracting Officer, the Contractor shall not commence work until a fully executed Task Order has been awarded. The Contractor may incur costs under this contract in performance of task orders and task order modifications issued in accordance with this ARTICLE. No other costs are authorized unless otherwise specified in the contract or expressly authorized by the Contracting Officer. The attached NIHBPSSII Standard Operating Procedures outline the processes for award of a NIHBPSSII task order.

b. Requesting Task Order Proposals.

The Contracting Officer or a designated individual may solicit responses to requirements from Contractors within a technical area covered by a task order requirement in writing. A Task Order Request for Proposals (TORFP) will be prepared and issued for each task order requirement.

Generally, the Task Order Request for Proposal (TORFP) will include but is not limited to the following:

1. Statement of Work;
2. Reporting Requirements and Deliverables;
3. Proposal Due Date and Location to Deliver Proposals;
4. Period of Performance of Task Order;
5. Anticipated type of Task Order;
6. Technical Proposal Instructions;
7. Business proposal Instructions
8. Evaluation Factors for Award

All contract clauses contained this contract shall be incorporated in the TORFP and the resultant task order. If conflicts exist between the contract clauses and the information outlined in the task order, the contract language takes precedence over the information in the task order.

Contractors are not required to propose on all TORFPs. Those eligible Contractors that decide not to submit a proposal shall advise the Contracting Officer, in writing, of their intention not to submit a proposal on or before the closing date and time established in the TORFP. An election not to propose on a given TORFP will not negatively affect or prohibit a Contractor from competing on future TORFPs. However, it may affect the Contractor's eligibility for continuations or extensions of the resultant Task Order.

c. Competitive Ordering Process.

1. All Contractors within a technical area will receive e-mail notification advising of the availability of each proposed task order requirement. All proposed task orders will incorporate all terms of this contract unless otherwise specified in the proposed task order.
2. Contractors will be provided an adequate time to prepare and submit responses based on the Contracting Officer's consideration of the estimated dollar value and complexity of proposed task order. Responses will not be considered a proposal as defined in FAR Part 15. However, the Contractor shall provide information sufficient for consideration in accordance with FAR Part 16. Each TORFP will indicate the criteria for the evaluation of proposals. The responses shall demonstrate capability for each criterion to be evaluated. Generally, the Contractor will be asked to demonstrate the following as appropriate:
 - Understanding of the requirements;
 - Experience and capability on similar tasks;
 - Technical approach, methods and procedures for satisfying the requirements with a discussion of potential problems to be encountered and proposed solutions and/or risk mitigation strategies.
 - Procedures for assuring quality of work, products, and deliverables;
 - Plan for managing the task order, including meeting requirements and schedules, and performance measures (if applicable);

- Staffing plan with skill levels and level of effort for each individual proposed. Generally, resumes will be required for proposed personnel (if not previously submitted);
- References to evaluate past performance; and
- Cost/Price to perform the task order.

d. Evaluation and Award of Task Order Proposals

The Government will evaluate the Task Order proposals against the requirements of the TORP. Specifically, the technical evaluation factors, cost/price, past performance and any other factor specifically identified in the TORP will be used for evaluation of each proposal. In addition, the TORP will identify the basis for selecting a contractor for award. Generally, technical factors will be significantly more important than cost or price. However, each TORP will specify how the award decision will be made.

Upon completion of evaluations, the Contracting Officer will issue a task order to the Contractor whose proposal is most advantageous to the government.

The Contracting Officer will notify the Contractor(s) of the selection decision in writing.

e. Fair Opportunity

1. In accordance with FAR 16.505(b)(1)(i), each awardee will be given a fair opportunity to be considered for each order exceeding the micro-purchase threshold issued under multiple delivery-order contracts or multiple task-order contracts, except:
 - i. The agency need for the supplies or services is so urgent that providing a fair opportunity would result in unacceptable delays.
 - ii. Only one awardee is capable of providing the supplies or services required at the level of quality required because the supplies or services ordered are unique or highly specialized.
 - iii. The order must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order.
 - iv. It is necessary to place an order to satisfy a minimum guarantee.
2. All awardees will be given a fair opportunity to be considered in accordance with the FAR as follows:
 - i. For orders exceeding the micro-purchase threshold up to the simplified acquisition threshold, in accordance with FAR 16.505(b)(1)(ii);
 - ii. For orders exceeding the simplified acquisition threshold up to \$6 Million, in accordance with 16.505(b)(1)(iii); and,
 - iii. For orders exceeding \$6 Million, in accordance with FAR 16.505(b)(1)(iv).

ARTICLE G.5. INVOICE SUBMISSION

a. Invoice Requirements

An invoice is the Contractor's bill or written request for payment under the contract for supplies delivered or services performed. A proper invoice is an "Original" which must include the items listed in subdivisions 1 through 12, below, in addition to the requirements of FAR 32.9. If the invoice does not comply with these requirements, the Contractor will be notified of the defect within 7 days after the date the designated billing office received the invoice (3 days for meat, meat food products, or fish, and 5 days for perishable agricultural commodities, dairy products, edible fats, or oils) with a statement of the reasons why it is not a proper invoice. (See exceptions under II., below.) Untimely notification will be considered in the computation

of any interest penalty owed the Contractor.

1. Vendor/Contractor: Name, Address, Point of Contact for the invoice (Name, title, telephone number, e-mail and mailing address of point of contact).
2. Remit-to address (Name and complete mailing address to send payment).
3. Remittance name must match exactly with name on original order/contract. If the Remittance name differs from the Legal Business Name, then both names must appear on the invoice.
4. Invoice date.
5. Unique invoice #s for all invoices per vendor regardless of site.
6. NBS document number formats must be included for awards created in the NBS: Contract Number; Purchase Order Number; Task or Delivery Order Number and Source Award Number (e.g., Indefinite Delivery Contract number; General Services Administration number); or, BPA Call Number and BPA Parent Award Number.
7. Unique Entity Identifier (UEI) which is in the System for Award Management (SAM) and replaces the Dun & Bradstreet Data Universal Numbering System (DUNS) number.
8. Federal Taxpayer Identification Number (TIN). In those rare cases where a contractor does not have a UEI number or TIN, a Vendor Identification Number (VIN) must be referenced on the invoice. The VIN is the number that appears after the contractor's name on the face page of the award document.
9. Identify that payment is to be made using a three-way match.
10. Description of supplies/services **that match** the description on the award, by line billed.*
11. Freight or delivery charge must be billed as shown on the award. If it is included in the item price do not bill it separately. If identified in the award as a separate line item, it must be billed separately.
12. Quantity, Unit of Measure, Unit Price, Extended Price of supplies delivered or services performed, as applicable, and that **match** the line items specified in the award.*

NOTE: If your invoice must differ from the line items on the award, please contact the Contracting Officer before submitting the invoice. A modification to the order or contract may be needed before the invoice can be submitted and paid.

Shipping costs will be reimbursed only if authorized by the Contract/Purchase Order. If authorized, shipping costs must be itemized. Where shipping costs exceed \$100, the invoice must be supported by a bill of lading or a paid carrier's receipt.

13. The Contractor shall submit invoices to the Department of Treasury's Invoice Processing Platform (IPP) at <https://www.ipp.gov> with a copy to the approving official, as directed below.

The Contractor shall submit a copy of the electronic invoice to the task order Approving Official (Contracting Officer) and Contracting Officer's Representative:

b. Invoice Payment

1. Except as indicated in paragraph B., below, the due date for making invoice payments by the designated payment office shall be the later of the following two events:
 2. The 30th day after the designated billing office has received a proper invoice.
 3. The 30th day after Government acceptance of supplies delivered or services performed.
4. The due date for making invoice payments for meat and meat food products, perishable agricultural commodities, dairy products, and edible fats or oils, shall be in accordance with the Prompt Payment Act, as amended.

c. Interest Penalties

1. An interest penalty shall be paid automatically, if payment is not made by the due date and the conditions listed below are met, if applicable.
2. A proper invoice was received by the designated billing office.
3. A receiving report or other Government documentation authorizing payment was processed and there was no disagreement over quantity, quality, or contractor compliance with a term or condition.

4. In the case of a final invoice for any balance of funds due the contractor for supplies delivered or services performed, the amount was not subject to further settlement actions between the Government and the Contractor.
5. Determination of interest and penalties due will be made in accordance with the provisions of the Prompt Payment Act, as amended, the Contract Disputes Act, and regulations issued by the Office of Management and Budget.

ARTICLE G.6. PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS, FAR 52.232-40 (December 2013)

- a. Upon receipt of accelerated payments from the Government, the Contractor shall make accelerated payments to its small business subcontractors under this contract, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, after receipt of a proper invoice and all other required documentation from the small business subcontractor.
- b. The acceleration of payments under this clause does not provide any new rights under the prompt Payment Act.
- c. Include the substance of this clause, include this paragraph c, in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of Clause)

ARTICLE G.7. GOVERNMENT PROPERTY

If task orders awarded under this contract will result in the acquisition or use of Government Property provided by the contracting agency, this ARTICLE incorporates the HHS Publication, entitled, "HHS Contracting Guide for Contract of Government Property," which can be found at: http://oamp.od.nih.gov/sites/default/files/appendix_q_hhs_contracting_guide.pdf.

It is not anticipated that GFP will be provided at the master contract level; however, GFP may be furnished under awarded tasks.

ARTICLE G.8. ON-SITE CONTRACTOR ACCESS TO GOVERNMENT PROPERTY

The Contractor shall be held responsible for Government Property, regardless of dollar value, when:

- The contract requires contractor personnel to be located on a Government site or installation;
- The property utilized by contractor personnel is incidental to the place of performance; and,
- The property used by the contractor remains accountable to the Government

Responsibility includes physical presence, proper use and handling, normal maintenance, and reporting loss, damage or destruction.

Responsibility for government property shared by two or more contractors or located in space shared by two or more contractors, shall be determined and documented by the contractors involved. In cases where the parties cannot reach agreement on shared responsibility, the matter will be referred to the NIH Property Officer for resolution.

ARTICLE G.9. POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE

- a. Contractor Performance Evaluations

Interim and Final evaluations of Contractor performance will be prepared on this contract in accordance with FAR Subpart 42.15. The Final performance evaluation will be prepared at the time of completion of work. In addition to the Final evaluation, Interim evaluation(s) will be prepared Annually as follows on To be completed at award [Insert Dates].

Interim and Final evaluations will be provided to the Contractor as soon as practicable after completion of the evaluation. The Contractor will be permitted thirty days to review the document and to submit additional information or a rebutting statement. If agreement cannot be reached between the parties, the matter will be referred to an individual one level above the Contracting Officer, whose decision will be final.

Copies of the evaluations, Contractor responses, and review comments, if any, will be retained as part of the contract file, and may be used to support future award decisions.

b. Electronic Access to Contractor Performance Evaluations

Contractors may access evaluations through a secure Web site for review and comment at the following address:

<http://www.cpars.gov>

SECTION H - SPECIAL CONTRACT REQUIREMENTS

ARTICLE H.1. HUMAN SUBJECTS

It is hereby understood and agreed that research involving human subjects shall not be conducted under this contract, and that no material developed, modified, or delivered by or to the Government under this contract, or any subsequent modification of such material, will be used by the Contractor or made available by the Contractor for use by anyone other than the Government, for experimental or therapeutic use involving humans without the prior written approval of the Contracting Officer.

ARTICLE H.2. ACKNOWLEDGEMENT OF FEDERAL FUNDING

The Contractor shall clearly state, when issuing statements, press releases, requests for proposals, bid solicitations and other documents describing projects or programs funded in whole or in part with Federal money: (1) the percentage of the total costs of the program or project which will be financed with Federal money; (2) the dollar amount of Federal funds for the project or program; and (3) the percentage and dollar amount of the total costs of the project or program that will be financed by nongovernmental sources.

ARTICLE H.3. DISSEMINATION OF FALSE OR DELIBERATELY MISLEADING INFORMATION

The Contractor shall not use contract funds to disseminate information that is deliberately false or misleading.

ARTICLE H.4. PRIVACY ACT, HHSAR 352.224-70 (December 2015)

This contract requires the Contractor to perform one or more of the following: (a) Design; (b) develop; or (c) operate a Federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) (5 U.S.C. 552a(m)(1)) and applicable agency regulations.

The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties (5 U.S.C. 552a(i)).

The Contractor shall ensure that each of its employees knows the prescribed rules of conduct in CFR 45 part 5b and that each employee is aware that he/she is subject to criminal penalties for violation of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under this contract which require the design, development or operation of the designated system(s) of records [5 U.S.C. 552a(m)(1)]. The contract work statement:

- (a) identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and
- (b) specifies the disposition to be made of such records upon completion of contract performance.

ARTICLE H.5. OMB CLEARANCE

In accordance with HHSAR 352.211-3, Paperwork Reduction Act, the Contractor shall not proceed with surveys or interviews until such time as Office of Management and Budget (OMB) Clearance for conducting interviews has been obtained by the Contracting Officer's Representative (COR) and the Contracting Officer has issued written approval to proceed.

ARTICLE H.6. RESTRICTION ON PORNOGRAPHY ON COMPUTER NETWORKS

The Contractor shall not use contract funds to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography.

ARTICLE H.7. GUN CONTROL

The Contractor shall not use contract funds in whole or in part, to advocate or promote gun control.

ARTICLE H.8. OPTION PROVISION

Unless the Government exercises its option pursuant to the Option Clause set forth in SECTION I., the contract will consist only of the Base Period of the Statement of Work as defined in Sections C and F of the contract. Pursuant to FAR Clause 52.217-9, Option to Extend the Term of the Contract set forth in SECTION I of this contract, the Government may, by unilateral contract modification, require the Contractor to perform additional options as defined in Sections C and F of the contract. If the Government exercises this option, notice must be given at least 60 days prior to the expiration date of this contract, and the price of the contract will be increased as set forth in the PRICE/COST Article in SECTION B of this contract.

Pursuant to FAR Clause 52.217-8, Option to Extend Services FAR Clause set forth in SECTION I of this contract, the Government may also, by unilateral contract modification, require the Contractor to perform additional options as defined in Sections C and F of the contract. If the Government exercises this option, notice must be given at least 14 days prior to the expiration date of this contract.

ARTICLE H.9. SUBCONTRACTING PROVISIONS

a. Small Business Subcontracting Plan

1. The Small Business Subcontracting Plan, dated TBD is attached hereto and made a part of this contract.
2. The failure of any Contractor or subcontractor to comply in good faith with FAR Clause 52.219-8, entitled "Utilization of Small Business Concerns" incorporated in this contract and the attached Subcontracting Plan, will be a material breach of such contract or subcontract and subject to the remedies reserved to the Government under FAR Clause 52.219-16 entitled, "Liquidated Damages-Subcontracting Plan."

b. Subcontracting Reports

The Contractor shall submit the following Subcontracting reports electronically via the "electronic Subcontracting Reporting System (eSRS) at <http://www.esrs.gov>.

1. Individual Subcontract Reports (ISR)

Regardless of the effective date of this contract, the Report shall be due on the following dates for the entire life of this contract:

April 30th
October 30th
Expiration Date of Contract

2. Summary Subcontract Report (SSR)

Regardless of the effective date of this contract, the Summary Subcontract Report shall be submitted annually on the following date for the entire life of this contract:

October 30th

For both the Individual and Summary Subcontract Reports, the Contracting Officer shall be included as a contact for notification purposes at the following e-mail address:

NIHBPSS@mail.nih.gov

ARTICLE H.10. HHS SECURITY AND PRIVACY LANGUAGE FOR INFORMATION AND IT PROCUREMENTS

The requirements in ARTICLES H.10.X shall be followed where applicable to the task order scope of work. Fill-ins will be addressed at the task order level.

ARTICLE H.10.1. INFORMATION SECURITY AND/OR PHYSICAL ACCESS SECURITY

A. Baseline Security Requirements

1. **Applicability-** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:
 - a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
 - b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
2. **Safeguarding Information and Information Systems-** In accordance with the Federal Information Processing Standards Publication (FIPS)199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:
 - a. Protect government information and information systems in order to ensure:
 - **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
 - **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
 - **Availability**, which means ensuring timely and reliable access to and use of information.
 - b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, **within one (1) hour or less**, bring the situation to the attention of the other party.
 - c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the HHS Information Security Program security requirements,

outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

d. Comply with the Privacy Act requirements.

3. **Information Security Categorization-** In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Contractor Non-Disclosure Agreement and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality: Low Moderate High
 Integrity: Low Moderate High
 Availability: Low Moderate High
 Overall Risk Level: Low Moderate High

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

No PII Yes PII

Personally Identifiable Information (PII). Per the Office of Management and Budget (OMB) Circular A-130, "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.

PII Confidentiality Impact Level has been determined to be: Low Moderate High

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

- a. Marked appropriately;
- b. Disclosed to authorized personnel on a Need-To-Know basis;
- c. Protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and
- d. Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

5. **Protection of Sensitive Information-** For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, Protection of Sensitive Agency Information by securing it with a FIPS 140-2 validated solution.
6. **Confidentiality and Nondisclosure of Information-** Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

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

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

Each employee, including subcontractors, having access to non-public Department information under this acquisition shall complete the "Commitment to Protect Non-Public Information - Contractor Employee Agreement" located at: <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf>. A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer/COR prior to performing any work under this acquisition.

7. **Internet Protocol Version 6 (IPv6)-** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6).
8. **Government Websites-** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.
9. **Contract Documentation-** The Contractor shall use provided templates, policies, forms and other agency documents provided by the Contracting Officer and the Contracting Officer's Representative to comply with contract deliverables as appropriate.
10. **Standard for Encryption-** The Contractor (and/or any subcontractor) shall:
 - a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.
 - b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.
 - c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and NIH-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

- d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the Contracting Officer and the Contracting Officer's Technical Representative within **15 days** of the validation .
 - e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.
11. **Contractor Non-Disclosure Agreement (NDA)**- Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the NIH non-disclosure agreement <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf>, as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
 12. **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)**- The Contractor shall assist the NIH Office of the Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed. The NIH PIA guide is located at <https://oma.od.nih.gov/forms/Privacy%20Documents/Documents/NIH%20PIA%20Guide.pdf> .
 - a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the OpDiv SOP or designee with completing a PIA for the system or information within **60 days** after completion of the PTA and in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
 - b. The Contractor shall assist the NIH Office of the SOP or designee in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

B. TRAINING

1. **Mandatory Training for All Contractor Staff**- All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/NIH Contractor Information Security Awareness, Privacy, and Records Management training course at <http://irtsectraining.nih.gov/> before performing any work under this contract. Thereafter, the employees shall complete NIH Information Security Awareness, Privacy, and Records Management training at least annually, during the life of this contract. All provided training shall be compliant with HHS training policies.
2. **Role-based Training**- All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training annually commensurate with their role and responsibilities in accordance with HHS policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum. Read further guidance about the NIH Role-based Training <https://ocio.nih.gov/aboutus/publicinfosecurity/securitytraining/Pages/rolebasedtraining.aspx>
3. **Training Records**- The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records shall be provided to the CO and/or COR within 30 days after contract award and **annually** thereafter or upon request.

C. RULES OF BEHAVIOR

1. The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the HHS Information Technology General Rules of Behavior, and comply with the NIH Information Technology General Rules of Behavior <https://ocio.nih.gov/InfoSecurity/training/Pages/nihitrob.aspx>, which are contained in the NIH Information Security Awareness Training Course <http://irtsectraining.nih.gov>
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 NIH Information Security Awareness Training. If the training is provided by the contractor, the signed Rules of Behavior must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

D. INCIDENT RESPONSE

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

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines incidents as events involving cyber security and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII" .

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

1. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.
2. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send NIH approved notifications to affected individuals in accordance with https://ocio.nih.gov/InfoSecurity/IncidentResponse/Pages/ir_guidelines.aspx
3. Report all suspected and confirmed information security and privacy incidents and breaches to the NIH Incident Response Team (IRT) via email at IRT@mail.nih.gov, COR, CO, the NIH Office of the SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than one (1) hour, and consistent with the applicable NIH 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, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

- a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
 - b. not include any sensitive information in the subject or body of any reporting e-mail; and
 - c. encrypt sensitive information in attachments to email, media, etc.
4. Comply with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information HHS and NIH incident response policies when handling PII breaches.
 5. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation within an hour of discovery.

E. POSITION SENSITIVITY DESIGNATIONS

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

[] Level 6: Public Trust - High Risk. Contractor/subcontractor employees assigned to Level 6 positions shall undergo a Suitability Determination and Background Investigation (MBI).

[] Level 5: Public Trust - Moderate Risk. Contractor/subcontractor employees assigned to Level 5 positions with no previous investigation and approval shall undergo a Suitability Determination and a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI).

[] Level 1: Non-Sensitive. Contractor/subcontractor employees assigned to Level 1 positions shall undergo a Suitability Determination and National Check and Inquiry Investigation (NACI).

F. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-12

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

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

Roster-

- a. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within fourteen (14) calendar days after the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within seven (7) calendar days of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for contractor use at: https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/SuitabilityRoster_10-15-12.xlsx.
- b. If the Contractor is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification.
- c. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification.
- d. The Contractor shall notify the Contracting Officer in advance when any new personnel, who are subject to a background check/investigation, will work under the contract and if they have previously been the subject of national agency checks or background investigations.
- e. All contractor and subcontractor employees shall comply with the conditions established for their designated position sensitivity level prior to performing any work under this contract. Contractors may begin work after the fingerprint check has been completed.
- f. Investigations are expensive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with the FAR clause, Excusable Delays - see FAR 52.249-14. Accordingly, the Contractor shall ensure that any additional employees whose names it submits for work under this contract have a reasonable chance for approval.
- g. Typically, the Government investigates personnel at no cost to the Contractor. However, 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 additional investigation(s).
- h. The Contractor shall include language similar to this "HHS Controlled Facilities and Information Systems Security" language in all subcontracts that require subcontractor personnel to have the same frequency and duration of (1) physical access to an HHS-controlled facility; (2) logical access to an HHS-controlled information system; (3) access to sensitive HHS data/information, whether in an HHS-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3).
- i. The Contractor shall direct inquiries, including requests for forms and assistance, to the Contracting Officer or designee.
- j. Within 7 calendar days after the Government's final acceptance of the work under this contract, or upon termination of the contract, the Contractor shall return all identification badges to the Contracting Officer or designee.

G. CONTRACT INITIATION AND EXPIRATION

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

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

2. **System Documentation-** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
3. **Sanitization of Government Files and Information-** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation in accordance with the NIH Media Sanitization and Disposal Policy to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.
4. **Notification-** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within **fifteen days** before an employee stops working under this contract.
5. **Contractor Responsibilities Upon Physical Completion of the Contract-** The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or NIH policies.
6. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the NIH Contractor Employee Separation Checklist <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Emp-sep-checklist.pdf> when an employee terminates work under this contract within 2 days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. RECORDS MANAGEMENT AND RETENTION

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/NIH policies and shall not dispose of any records unless authorized by HHS/NIH. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/NIH policies.

ARTICLE H.10.2. 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 on individuals.

The System of Records Notice (SORN) that is applicable to this contract is: _____ [*Insert SORN number if one exists. If there is no SORN, indicate that a SORN will be developed*].

The design, development, or operation work the Contractor is to perform is: _____ [*Insert description of design, development, and/or operation work; see definitions in the FAR at 24.101 - Definitions*].

The Contractor and any Subcontractor must follow disposition to be made of the Privacy Act records upon completion of contract performance shall be in accordance with Section C of the contract, and by direction of the Contracting Officer/Contracting Officer's representative.

ARTICLE H.10.3. GOVERNMENT INFORMATION PROCESSED ON GOCO OR COCO SYSTEMS

A. SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED/CONTRACTOR-OPERATED (GOCO)AND CONTRACTOR-OWNED/CONTRACTOR-OPERATED (COCO) RESOURCES

1. **Federal Policies-** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the HHS Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
2. **Security Assessment and Authorization (SA&A)-** A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) within three (3) months after contract award. The Contractor shall conduct the SA&A requirements in accordance with HHS IS2P, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (latest revision).

For an existing ATO, Contracting Officer Representative must make a determination if the existing ATO provides appropriate safeguards or if an additional ATO is required for the performance of the contract and state as such.

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

- a. **SA&A Package Deliverables -** The Contractor (and/or any subcontractor) shall provide an SA&A package within 30 days of contract award to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package.
 - **System Security Plan (SSP) -** due within 30 days after contract award. The SSP shall comply with the NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the Federal Information Processing Standard (FIPS) 200, Recommended Security Controls for Federal Information Systems, and NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable

baseline requirements, and other applicable NIST guidance as well as HHS and NIH policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least annually thereafter.

- **Security Assessment Plan/Report (SAP/SAR)** - due 30 days after the contract award. The security assessment shall be conducted by the assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and NIH policies. The assessor will document the assessment results in the SAR.

The NIH should determine which security control baseline applies and then make a determination on the appropriateness/necessity of obtaining an independent assessment. Assessments of controls can be performed by contractor, government, or third parties, with third party verification considered the strongest. If independent assessment is required, include statement below.

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

- **Independent Assessment** - due 90 days after the contract award. The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). 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. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).
- **POA&M** - due 30 days after contract award. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and NIH policies. All high-risk weaknesses must be mitigated within 30 days and all medium weaknesses must be mitigated within 60 days from the date the weaknesses are formally identified and documented. The NIH will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, NIH may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least quarterly.
- **Contingency Plan and Contingency Plan Test** - due 60 days after contract award. 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 NIH policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least annually.
- **E-Authentication Questionnaire** - The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

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

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

(ISCM) for Federal Information Systems and Organizations, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/Pen Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date provided by the Contracting Officer's Representative.
 - **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 60 days after contract award. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
 - **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least within 60 days. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
 - **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least within 60 days. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
 - **Vulnerability Management** - Use SCAP-compliant automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least within 30 days of the contract award.
 - **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.
 - **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
1. **Government Access for Security Assessment.** In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability

of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:

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

The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

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

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

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

- a. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-2 encryption standards.

- b. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), and HHS Minimum Security Configuration Standards;
- c. Maintain the latest operating system patch release and anti-virus software definitions within 15 days.
- d. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
- e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
 - Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
 - Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

ARTICLE H.10.4. CLOUD SERVICES

A. HHS FedRAMP Privacy and Security Requirements

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

- a. **FedRAMP Compliant ATO.** Comply with FedRAMP Security Assessment and Authorization (SA&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 shall submit a plan to obtain a FedRAMP compliant ATO by 30 days of the contract award.
 - b. 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.
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 (CONUS) if so required as stated in section C.
3. **Service Level Agreements-** Add when applicable/Mark as Not Applicable_____The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with NIH to develop and maintain an SLA.

4. **Interconnection Agreements/Memorandum of Agreements-** Add when applicable/Mark as Not Applicable _____ The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/NIH policies.

B. Protection of Information in a Cloud Environment

1. If contractor (and/or any subcontractor) personnel must 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/NIH policies.
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 shall be provided at no additional cost to HHS.
3. The Contractor (and/or any subcontractor) 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 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:
 - a. Maintenance of links between records and metadata, and
 - b. 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 HHS/NIH. 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.
6. 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.

C. Security Assessment and Authorization (SA&A) Process

1. The Contractor (and/or any subcontractor) shall 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 SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/NIH security policies.
 - a. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the NIH authorizing official (AO) prior to implementation of system and/or service being acquired.

- b. 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. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
 - c. For all acquired cloud services, the SA&A package must contain the following documentation: SSP, SAR, POA&M, Authorization Letter, CP and CPT report, E-Authorization (if applicable), PTA/PIA (if applicable), Interconnection/Data Use Agreements (if applicable), 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/NIH policies.
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) 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, 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.
 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, all gaps shall be documented and tracked by the contractor 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 (and/or any subcontractor) shall mitigate security risks for which they are responsible, including those identified during SA&A and continuous monitoring activities. All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery: (1) critical vulnerabilities no later than thirty (30) days and (2) high, medium and low vulnerabilities no later than sixty (60) days. In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they shall be added to the designated POA&M and mitigated within the newly designated timelines 30 days. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.
 5. Revocation of a Cloud Service. HHS/NIH staff division 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 NIH 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.

D. Reporting and Continuous Monitoring

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.

Information Security Continuous Monitoring- Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements

in accordance with FISMA and NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/Pen Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date provided by the Contracting Officer's Representative.
 - **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 60 days after contract award. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
 - **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least within 60 days. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
 - **Vulnerability Management** - Use SCAP-compliant automated tools for authenticated scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least within 30 days of the contract award.
 - **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.
 - **Secure Coding** - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - **Boundary Protection** - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
 - 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.
2. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis as directed by the Contracting Officer/Contracting Officer's Representative.
- a. Operating system, database, Web application, and network vulnerability scan results;
 - b. Updated POA&Ms;
 - c. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the NIH System Owner or AO; and

- d. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/NIH's 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.

E. Configuration Baseline

1. The contractor shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/NIH.
 - The Contractor shall configure its computers that contain HHS data with the latest applicable United States Government Configuration Baseline (USGCB) and/or other approved HHS IT Security Configurations. (See: <https://usgcb.nist.gov/>). Note: Approved security configurations include, but are not limited to, those published by the Department, the NIH , and the National Institute of Standards and Technology (NIST) . NIH may have security configurations that are more stringent than the minimum baseline set by the Department or NIST. When incorporating such security configuration requirements in solicitations and contracts, the NIH CISO and/or Information System Security Officer (ISSO) shall be consulted to determine the appropriate configuration reference for a particular system or services acquisition.)
 - The Contractor shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS and must adhere to all NIH configuration standards and policies (See: <https://ocio.nih.gov/InfoSecurity/Policy/Pages/CM.aspx>).
 - The Contractor shall ensure IT applications operated on behalf of HHS are fully functional and operate correctly on systems configured in accordance with the above configuration requirements. The Contractor shall use Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capability to ensure its products operate correctly with USGCB configurations and do not alter USCGB settings - (See: <http://scap.nist.gov/validation>) . The Contractor shall test applicable product versions with all relevant and current updates and patches installed. The Contractor shall ensure currently supported versions of information technology products met the latest USGCB major version and subsequent major versions.
 - The Contractor shall ensure IT applications designed for end users run in the standard user context without requiring elevated administrative privileges.
 - The Contractor shall ensure hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above.
 - The Contractor shall (1) include Federal Information Processing Standard (FIPS) 201-compliant (See: <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>), Homeland Security Presidential Directive 12 (HSPD-12) card readers with the purchase of servers, desktops, and laptops; and (2) comply with FAR Subpart 4.13, Personal Identity Verification.
 - The Contractor shall ensure that its subcontractors (at all tiers) which perform work under this contract comply with the requirements contained in this clause.
2. The contractor shall 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.

F. Incident Reporting

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

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines incidents as events involving cyber security and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII" .

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

1. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.
2. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send NIH approved notifications to affected individuals within **5 business days** of the incident.
3. Report all suspected and confirmed information security and privacy incidents and breaches to the NIH Incident Response Team (IRT) IRT@nih.gov, COR, CO, the NIH Office of the SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than one (1) hour, and consistent with the applicable NIH 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, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:
 - a. Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
 - b. Not include any sensitive information in the subject or body of any reporting e-mail; and
 - c. Encrypt sensitive information in attachments to email, media, etc
4. Comply with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information HHS and NIH incident response policies when handling PII breaches.
5. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.
6. The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS/NIH, OMB, and US-CERT requirements and obtain approval from the NIH. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
7. 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 shall include, but is not limited to:

- a. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/NIH personnel, or agents acting on behalf of HHS/NIH, 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.
- b. 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.

G. Media Transport

1. The Contractor and its employees 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).
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.

H. 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 Trusted Internet Connection (TIC) processes.
2. The contractor shall route all external connections through a TIC.
3. **Non-Repudiation-** The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

ARTICLE H.10.5. OTHER IT PROCUREMENTS

ARTICLE H.10.5.1. NON-COMMERCIAL AND OPEN SOURCE COMPUTER SOFTWARE

The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by the 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.

ARTICLE H.10.5.2. INFORMATION TECHNOLOGY APPLICATION DESIGN, DEVELOPMENT, OR SUPPORT

1. The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
2. The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
3. The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data shall be used during software testing.
4. The Contractor (and/or any subcontractor) shall protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

ARTICLE H.10.5.3. PHYSICAL ACCESS TO GOVERNMENT CONTROLLED FACILITIES

Refer to section H clause- Government Information and Physical Access Security.

ARTICLE H.11. ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY NOTICE HHSAR 352.239-73 (December 2015)

- a. a. Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 and the Architectural and Transportation Barriers Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain,

or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

- b. b. Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at <http://www.hhs.gov/web/508> . The complete text of the Section 508 Final Provisions can be accessed at <http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards> .
- c. c. The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-74, Electronic and Information Technology Accessibility. In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document--in detail--whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site <http://www.hhs.gov/web/508> . In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.
- d. d. Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.
- The "HHS Section 508 Product Assessment Template" is included in SECTION J - List of Attachments, of this solicitation.

ARTICLE H.12. COMMUNICATIONS MATERIALS AND SERVICES

To build and maintain public trust; promote credibility and consistency; minimize consistency and frustration; and contribute to efforts aimed at leveraging reduced resources and eliminating waste in Government, the Contractor shall ensure that all materials generated and/or services provided under this contract, comply with all applicable NIH policy and procedures published by the NIH Office of Management Assessment in conjunction with the NIH Office of Communications and Public Liaison as set forth below.

This acquisition may require the contractor to:

[X] Prepare, review, and/or distribute NIH Publications and Audiovisuals.

NIH Policy Manual Chapter 1183, "NIH Publications & Audiovisuals: Preparation, Review, Approval & Distribution," is applicable to this contract. <http://oma1.od.nih.gov/manualchapters/management/1183/>.

[X] Use the NIH name and logo.

NIH Policy Manual Chapter 1186, "Use of NIH Names and Logos," is applicable to this contract. <http://oma1.od.nih.gov/manualchapters/management/1186/>.

[X] Create and/or Manage a Public Website which includes NIH hosted social media site(s), Web

application(s) and mobile Web Site(s).

NIH Policy Manual Chapter 2804, "Public-Facing Web Management," is applicable to this contract. <http://oma1.od.nih.gov/manualchapters/management/2804/>.

[X] Create and/or Manage an NIH Website that maintains and disseminates personal information.

NIH Policy Manual Chapter 2805, "NIH Web Privacy Policy," is applicable to this contract. <http://oma1.od.nih.gov/manualchapters/management/2805/>.

[X] Create and/or Manage an NIH hosted and/or funded social media site(s), Web application(s) and mobile Web site(s).

NIH Policy Manual Chapter 2809, "NIH Social and New Media Policy," is applicable to this contract. <http://oma1.od.nih.gov/manualchapters/management/2809/>.

Additional Standards applicable to this contract are identified in the Statement of Work. If it is determined by the Government that products, services, and deliverables provided by the Contractor do not conform to standards described in these directives, remediation to an acceptable level of conformance shall be the responsibility of the Contractor at its own expense.

ARTICLE H.13. ACCESS TO NATIONAL INSTITUTES OF HEALTH (NIH) ELECTRONIC MAIL

All Contractor staff that have access to and use of NIH electronic mail (e-mail) must identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, the Contractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each Contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent.

ARTICLE H.14. CONTRACTOR'S USE OF LIBRARY RESOURCES AT NIH

The Contractor is authorized to use library resources at NIH in the same manner as NIH staff. The Contractor's approved use of these resources is limited to performing the requirements of this contract. The Contractor shall not use library resources at NIH in a manner that exceeds the Fair Use limitations codified in 17 U.S.C. sec. 107 of the Copyright Act. Contractors shall not share access to library resources at NIH with, perform searches for, or provide results to, non-NIH users, i.e. collaborators at other universities or research centers.

ARTICLE H.15. CONFIDENTIALITY OF INFORMATION

- a. Confidential information, as used in this article, 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. The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the Contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.
- c. If it is established elsewhere in this contract that information to be utilized under this contract, or a portion thereof, is subject to the Privacy Act, the Contractor will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.
- d. Confidential information, as defined in paragraph (a) of this article, shall not be disclosed without the prior written consent of the individual, institution, or organization.
- e. Whenever the Contractor is uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this article, the Contractor should obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

- f. Contracting Officer determinations will reflect the result of internal coordination with appropriate program and legal officials.
- g. The provisions of paragraph (d) of this article shall not apply to conflicting or overlapping provisions in other Federal, State or local laws.

The following information is covered by this article:

To be identified at the task order level, as necessary.

ARTICLE H.16. TASK ORDER/DELIVERY ORDER CONTRACT OMBUDSMAN

In accordance with FAR 16.505(b)(8), the following individual has been designated as the NIH Ombudsman for task order and delivery order contracts.

For Non R&D Contracts:
Dr. Richard G. Wyatt
NIH Competition Advocate
1 Center Drive, Room 160, MSC 0151
Bethesda, MD 20892-0151
Phone: (301) 496-4920
E-mail: WyattRG@mail.nih.gov

ARTICLE H.17. REPORTING MATTERS INVOLVING FRAUD, WASTE AND ABUSE

Anyone who becomes aware of the existence or apparent existence of fraud, waste and abuse in NIH funded programs is encouraged to report such matters to the HHS Inspector General's Office in writing or on the Inspector General's Hotline. The toll free number is **1-800-HHS-TIPS (1-800-447-8477)**. All telephone calls will be handled confidentially. The website to file a complaint on-line is: <http://oig.hhs.gov/fraud/hotline/> and the mailing address is:

US Department of Health and Human Services
 Office of Inspector General
 ATTN: OIG HOTLINE OPERATIONS
 P.O. Box 23489
 Washington, D.C. 20026

ARTICLE H.18. HOTEL AND MOTEL FIRE SAFETY ACT OF 1990 (P.L. 101-391)

Pursuant to Public Law 101-391, no Federal funds may be used to sponsor or fund in whole or in part a meeting, convention, conference or training seminar that is conducted in, or that otherwise uses the rooms, facilities, or services of a place of public accommodation that do not meet the requirements of the fire prevention and control guidelines as described in the Public Law. This restriction applies to public accommodations both foreign and domestic.

Public accommodations that meet the requirements can be accessed at: <http://apps.usfa.fema.gov/hotel/>.

ARTICLE H.19. CONSTITUTION DAY

Each educational institution that receives Federal funds for a fiscal year shall hold an educational program on the United States Constitution on September 17 of such year for the students serviced by the educational institution in accordance with Public Law 108-447.

ARTICLE H.20. USE OF FUNDS FOR CONFERENCES, MEETINGS AND FOOD

The Contractor shall not use contract funds (direct or indirect) to conduct meetings or conferences in performance of this contract without prior written Contracting Officer approval.

In addition, the use of contract funds to purchase food for meals, light refreshments, or beverages is expressly prohibited.

PART II - CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

The complete listing of these clauses may be accessed at:

<https://oamp.od.nih.gov/DGS/reference-material-prospective-offerors-and-contractors>

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

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

Alternate 1 (Jan 2017) is applicable to Time and Material and Labor Hour task orders

ARTICLE I.2. AUTHORIZED SUBSTITUTIONS OF CLAUSES

Any authorized substitutions and/or modifications other than the General Clauses which will be based on the type of contract/Contractor will be determined during negotiations.

It is expected that the following substitution(s) will be made part of the resultant contract:

- a. THERE ARE NO APPLICABLE CLAUSES IN THIS SECTION.

ARTICLE I.3. ADDITIONAL CONTRACT CLAUSES

Additional clauses other than those listed below which are based on the type of contract/Contractor shall be determined during negotiations. Any contract awarded from this solicitation will contain the following:

This contract incorporates the following clauses by reference, (unless otherwise noted), 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.

- a. FEDERAL ACQUISITION REGULATION (FAR) (48 CFR CHAPTER 1) CLAUSES

1. FAR Clause **52.204-9, Personal Identity Verification of Contractor Personnel** (January 2011).

2. FAR Clause **52.204-18 Commercial and Government Entity Code Maintenance** (July 2016)

3. FAR Clause **52.217-8, Option to Extend Services** (November 1999).

..The Contracting Officer may exercise the option by written notice to the Contractor within 14 days of contract expiration.

4. FAR Clause **52.224-1, Privacy Act Notification** (April 1984).

5. FAR Clause **52.224-2, Privacy Act** (April 1984).

6. FAR Clause **52.227-14, Rights in Data - General** (May 2014).

7. FAR Clause **52.237-2, Protection of Government Buildings, Equipment and Vegetation** (April 1984).

8. FAR Clause **52.245-1, Government Property** (Jan 2017).

b. DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CHAPTER 3) CLAUSES:

1. HHSAR Clause **352.208-70, Printing and Duplication** (December 2015)

2. HHSAR Clause **352.211-3, Paperwork Reduction Act** (December 2015)

3. HHSAR Clause **352.219-71, Mentor-Protégé Program Reporting Requirements** (December 2015).

4. HHSAR Clause **352.231-70, Salary Rate Limitation** (December 2015)

Note: *The Salary Rate Limitation is at the Executive Level II Rate.*

See the following website for Executive Schedule rates of pay: <https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/>.

(For current year rates, click on Salaries and Wages/Executive Schedule/Rates of Pay for the Executive Schedule. For prior year rates, click on Salaries and Wages/select Another Year at the top of the page/Executive Schedule/Rates of Pay for the Executive Schedule. Rates are effective January 1 of each calendar year unless otherwise noted.)

5. HHSAR **352.232-71 Electronic Submission of Payment Requests (February 2, 2022)**

(a) Definitions. As used in this clause—

Payment request means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must comply with the requirements identified in FAR 32.905(b), “Content of Invoices” and the applicable Payment clause included in this contract.

(b) Except as provided in paragraph (c) of this clause, the Contractor shall submit payment requests electronically using the Department of Treasury Invoice Processing Platform (IPP) or successor system. Information regarding IPP, including IPP Customer Support contact information, is available at www.ipp.gov or any successor site.

(c) The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing in accordance with HHS procedures.

(d) If alternate payment procedures are authorized, the Contractor shall include a copy of the Contracting Officer’s written authorization with each payment request.

(End of Clause)

ARTICLE I.4. ADDITIONAL FAR CONTRACT CLAUSES INCLUDED IN FULL TEXT

This contract incorporates the following clauses in full text.

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

1. FAR Clause 52.204-21, **Basic Safeguarding of Covered Contractor Information Systems** (June 2016)

a. *Definitions* . As used in this clause--

"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

"Safeguarding" means measures or controls that are prescribed to protect information systems.

b. Safeguarding requirements and procedures.

1. The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- i. Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- ii. Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- iii. Verify and control/limit connections to and use of external information systems.
- iv. Control information posted or processed on publicly accessible information systems.
- v. Identify information system users, processes acting on behalf of users, or devices.
- vi. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- vii. Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

- viii. Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- ix. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- x. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- xi. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- xii. Identify, report, and correct information and information system flaws in a timely manner.
- xiii. Provide protection from malicious code at appropriate locations within organizational information systems.
- xiv. Update malicious code protection mechanisms when new releases are available.
- xv. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

2. *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

c. *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

FAR Clause 52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Jul 2020)

- 2. (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 items:
 - (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 and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
 - (3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).
 - (4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)
 - (5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 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 items:

[Contracting Officer check as appropriate.]

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020) (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).

(4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (June 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

(6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

(7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

(8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020) (31 U.S.C. 6101 note).

(9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

(10) [Reserved]

(11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Mar 2020) (15 U.S.C. 657a).

(ii) Alternate I (Mar 2020) of 52.219-3.

(12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Mar 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

(ii) Alternate I (Mar 2020) of 52.219-4.

(13) [Reserved]

(14) (i) 52.219-6, Notice of Total Small Business Aside (Mar 2020) (15 U.S.C. 644).

(ii) Alternate I (Mar 2020).

(iii) Alternate II (Mar 2020).

(15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Mar 2020) (15 U.S.C. 644).

(ii) Alternate I (Mar 2020) of 52.219-7.

(16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

(17) (i) 52.219-9, Small Business Subcontracting Plan (Jan 2020) (15 U.S.C. 637 (d)(4)).

___(ii) Alternate I (Nov 2016) of 52.219-9.

X (iii) Alternate II (Nov 2016) of 52.219-9.

___(iv) Alternate III (Jun 2020) of 52.219-9.

___(v) Alternate IV (Jun 2020) of 52.219-9.

X (18) 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 (19) 52.219-14, Limitations on Subcontracting (Mar 2020) (15 U.S.C. 637(a)(14)).

X (20) 52.219-16, Liquidated Damages-Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

___(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Mar 2020) (15 U.S.C. 657f).

X (22) 52.219-28, Post Award Small Business Program Representation (May 2020) (15 U.S.C. 632(a)(2)).

___(23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Mar 2020) (15 U.S.C. 637(m)).

___(24) 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 (Mar 2020) (15 U.S.C. 637(m)).

X (25) 52.219-32, Order Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

X (26) 52.219-33, Nonmanufacturer Rule (Mar 2020) (15U.S.C. 637(a)(17)).

X (27) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

X (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2020) (E.O. 13126).

X (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

X (30) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

X (31) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

X (32) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

X (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

X (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (35) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (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 (36) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

___(37) (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.)

___(38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

___(39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

___(40) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514

___(ii) Alternate I (Oct 2015) of 52.223-13.

___(41) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

___(ii) Alternate I (Jun 2014) of 52.223-14.

___(42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).

X (43) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

___(ii) Alternate I (Jun 2014) of 52.223-16.

X (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Jun 2020) (E.O. 13513).

___(45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).

___(46) 52.223-21, Foams (Jun 2016) (E.O. 13696).

X (47) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

___(ii) Alternate I (Jan 2017) of 52.224-3.

___(48) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).

___(49) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 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 (May 2014) of 52.225-3.

___(iii) Alternate II (May 2014) of 52.225-3.

___(iv) Alternate III (May 2014) of 52.225-3.

X (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

X (51) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (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. 2302 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).

___(55) 52.229-12, Tax on Certain Foreign Procurements (Jun 2020).

___(56) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).

___(57) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

X (58) 52.232-33, Payment by Electronic Funds Transfer- System for Award Management (Oct 2018) (31 U.S.C. 3332).

___(59) 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

___(60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

X (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

X (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

___(63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

___(ii) Alternate I (Apr 2003) 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 items:

[Contracting Officer check as appropriate.]

___(1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)

___(2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).

___(3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___(4) 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).

___(5) 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).

___(6) 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).

___(7) 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).

___(8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).

___(9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

____(10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (Jun 2020) (42 U.S.C. 1792).

____(11) 52.237-11, Accepting and Dispensing of \$1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(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, 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 items. 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 (Jun 2020) (41 U.S.C. 3509).

(ii) 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)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (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 \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

(xi) 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.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).

(xiii)(A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (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 E.O. 13627).

(xiv) 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.)

(xv) 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)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

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

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 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. 2302 Note).

(xxi) 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.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) 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 items a minimal number of additional clauses necessary to satisfy its contractual obligations.

3. FAR Clause **52.216-18, Ordering** (October 1995).

- a. Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from _____ through _____. [To be completed at award for the Base year]
- b. All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.
- c. If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

4. FAR Clause **52.216-19, Order Limitations** (October 1995)

- a. **Minimum Order.** When the Government requires supplies or services covered by this contract in an amount of less than \$250, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.
- b. **Maximum Order.** The Contractor is not obligated to honor--
 - 1. Any order for a single item in excess of \$49,000,000.
 - 2. Any order for a combination of items in excess of \$49,000,000; or
 - 3. A series of orders from the same ordering office within 60 days that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.
- c. If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.
- d. Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 7 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

5. FAR Clause **52.216-22, Indefinite Quantity** (October 1995)

- a. This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
- b. Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."
- c. Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
- d. Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after August 12, 2025.

(End of clause)

6. FAR Clause **52.217-9, Option to Extend the Term of the Contract** (March 2000).

- a. The Government may extend the term of this contract by written notice to the Contractor within 7 days of contract expiration, provided that the Government gives the Contractor a preliminary

written notice of its intent to extend at least 60days 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 2 YEARS.

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

The following documents are attached and incorporated in this contract:

1. Statement of Work – NIHBPSSIII, dated July 24, 2020

2. Commitment to Protect Non-Public Information

Commitment To Protect Non-Public Information, 1 page. Located at: <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf>

3. Roster of Employees Requiring Suitability Investigations

Roster of Employees Requiring Suitability Investigations, 1 page. Excel file located at: https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/SuitabilityRoster_10-15-12.xlsx

4. Employee Separation Checklist

Employee Separation Checklist, 1 page. Fillable PDF format located at: <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Emp-sep-checklist.pdf>

PART IV - REPRESENTATIONS AND INSTRUCTIONS

SECTION K - REPRESENTATIONS AND CERTIFICATIONS

The following documents are incorporated by reference in this contract:

1. FAR Clause 52.204-19 **Incorporation by Reference of Representations and Certifications** (December 2014).

The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

END of the CONTRACT

SECTION C - STATEMENT OF WORK, dated 24 July 2020

1 Scope

Independently and not as an agent of the Government, the Contractor shall furnish all the necessary services, qualified personnel, material, equipment, and facilities, not otherwise provided by the Government as needed to perform the Statement of Work below:

2 Requirements

2.1 The contractor shall provide program management, project control, and contract administration necessary to manage the contract process so that cost, schedule, and quality requirements are tracked and communicated to the Contracting Officer's Representative (COR). The COR is located within the Category Management, Strategic Sourcing, and Data Analysis Branch (CMSSDA).

2.2 The contractor shall comply with all applicable federal standards, laws, codes, regulations policies, and statutes applicable to performance of this contract.

2.3 The contractor shall possess the following knowledge and experience:

- a. Familiarity with supply and property inventory policies.
- b. Understanding of supply management.
- c. Knowledge of property cataloging processes and data.
- d. Knowledge of financial accounting policies and financial tracking systems.
- e. Knowledge of SharePoint, SharePoint Designer, Visio, SPSS, and SAS.
- f. Experience in the design, development, and deployment of Dashboards and related tools.
- g. Experience with succession program management.
- h. Experience with workforce planning and development.
- i. Experience with instructional design, training management, and facilitation.
- j. Experience with business process improvement methodologies.
- k. Experience with organizational diagnosis and intervention techniques.
- l. Experience with human resources modeling, forecasting, needs analysis, and succession planning.

2.4 The contractor shall provide a Program Manager:

1. The Program Manager will be responsible for the overall performance objectives, contract deliverables, quality control (QC), and the placement of qualified personnel on this contract. The Program Manager will serve as the Contractor's authorized point of contact with NIH and shall ensure contract compliance and satisfactory performance.

2. This position requires a college degree and at least five (5) years of relevant experience

or a high school diploma and ten (10) years of relevant experience. Relevant experience required for this position involves program management performing tasks such as staffing, budgeting, scheduling, and client interaction. Experience in a scientific research or clinical environment or a Federal agency is preferred.

- 2.5 The contractor's Program Manager, or an appropriate designee, shall meet as requested with the COR to discuss task areas and any problems; and, to determine future tasks to be undertaken, meetings to be attended, and persons to be contacted on a weekly basis. The contractor shall record and forward to the COR any risks identified in the meeting, issues discussed in the meeting, the decisions rendered and the action items for each meeting member to address, within 5 working days after each meeting. This will include any risk handling activities and mitigation strategies.
- 2.6 The contractor's Program Manager, or an appropriate designee, shall attend relevant planning meetings, teleconferences, conferences, and forums as requested by the COR.
- 2.7 The contractor's Program Manager, or an appropriate designee, shall prepare meeting agendas, minutes, briefings, speeches, papers, letters, manuals, job aids, or other documents at the request of the COR.
- 2.8 The contractor's Program Manager, or an appropriate designee, shall design, develop, and deploy dashboards and related tools.
- 2.9 The contractor's Program Manager, or an appropriate designee, shall shall develop and maintain components of task project schedules for tracking the task/sub-tasks specifically identified by the COR. The contractor shall enter their portion of the task or sub-task project schedule into a database specified by the COR within 10 days of the start of a new task or sub-task. The contractor shall update the project schedule monthly with percentage of work completed, schedule date changes, or other schedule changes as requested by the COR.
- 2.10 The contractor's Program Manager, or an appropriate designee, shall shall prepare monthly status reports. Each status report shall provide the status of each task area that was worked on, or was scheduled to be worked on, during the reporting period. Each status report shall also document any problems encountered and how they were, or will be, resolved. Each report shall also document the contractor's plans for the next reporting period, including expected accomplishments, anticipated problems and projected solutions. The contractor shall deliver status reports by the tenth working day of each month following the first full month of task order performance.
- 2.11 The contractor's Program Manager, or an appropriate designee, shall will submit a written report on an annual basis detailing the work that has been accomplished.

3 Tasks Areas

3.1 Task Area 1: Financial Analysis, Business Solutions, and Acquisition Lifecycle Support

The contractor shall use existing Government financial systems and data, to conduct in depth financial analyses and make recommendations on financial improvements. The contractor shall provide a full range of acquisition support services at the request of the COR.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Provide financial and inventory management analytics.
- b. Provide support for logistics management activities, including, revenue forecasting, supply/demand analysis, and breakeven analysis.

- c. Work in collaboration with the COR to develop inventory, transportation, property, and other metrics.
- d. Provide support for traffic management, and data warehousing.
- e. Work in collaboration with the COR to track actual and budgeted costs.
- f. Work in collaboration with the COR to perform cost allocations.
- g. Work in collaboration with the COR to track supply chain activity costs.
- h. Work in collaboration with the COR to identify resource burdens and determine specific areas for improvement.
- i. Provide cradle to grave acquisition assistance for the full acquisition lifecycle, including pre-solicitation, contract administration and contract closeout support.

3.2 Task Area 2: Business Process Improvement and Organizational Assessment

The contractor shall work in collaboration with the COR to apply business process improvement methodologies, including Lean Six Sigma (LSS), in order to identify opportunities for process improvement initiatives and organizational and cultural change processes.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Work in collaboration with Government staff to develop the Strategic Plan.
- b. Work with the COR to identify, select, and align business process improvement projects to strategic objectives.
- c. Train NIH personnel in LSS, including Project Sponsor, Executive Awareness, Black Belt, Green Belt, and White Belt modules.
- d. Serve on a LSS certification board.
- e. Coach and mentor Black Belt, and Green Belt candidates through certification.
- f. Lead selected complex business process improvement efforts, including LSS projects, at the request of the COR.
- g. Conduct post LSS training evaluation and reinforcement projects.
- h. Lead LSS user groups, electronic forums, and brown bag sessions at the request of the COR.
- i. Conduct periodic LSS refresher training at the request of the COR.

3.3 Task Area 3: Communication and Training

The Contractor shall provide expert communications, outreach, and training support for external customers/users. Any applicable communications, outreach, and training materials will be provided to the Government in both paper and soft copy.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Work in collaboration with the COR to develop and implement an outreach strategy

and plan.

- b. Plan and conduct branding initiatives at the request of the COR.
- c. Work in collaboration with the COR to develop target messages and strategies.
- d. Plan and facilitate work sessions at the request of the COR.
- e. Work in collaboration with the COR to develop communication plans and supporting business cases.
- f. Work in collaboration with the COR in the selection of delivery methods (digital, print, live).
- g. Work in collaboration with the COR to develop communication designs, communication plans, implementation plans, and calendars; conduct communication reviews and evaluations.
- h. Work in collaboration with the COR to develop strategy, including prioritized needs based on mission; and timeframe/milestones.
- i. Work in collaboration with the COR to conduct in depth cost analyses.
- j. Work in collaboration with the COR to develop strategy-based metrics.

3.4 Task Area 4: Program Planning and Management Services

The Contractor shall provide program planning and management support at the request of the COR. The Contractor shall also provide performance management, and analytics and studies support.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Provide program planning, development and evaluation services.
- b. Provide workforce planning, resource management, and risk management support.
- c. Work in collaboration with the COR to develop, manage and evaluate the NIH Succession Management Program.
- d. Provide conference and meeting services.
- e. Provide project management support services.
- f. Provide tracking and monitoring support.
- g. Perform coordination activities.
- h. Provide survey services.
- i. Provide technical and advisory services for the purpose of COVID-19 efforts.

3.5 Task Area 5: Policy Development, Implementation, and Administration

The contractor shall provide written policy development support at the request of the COR.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Work in collaboration with the COR to identify policy needs, issues, and problems.
- b. Recommend policy actions and assist in policy implementation, administration, and oversight. Policy oversight shall include an evaluative component to ensure that policies accomplish established goals. Policies shall be stated with room for adjustment to fit special circumstances.
- c. Examine existing policies in order to make recommendations for revisions and improvements.
- d. Perform additional policy development tasks at the request of the COR.

3.6 Task Area 6: System Integration Work

The Contractor shall coordinate with all elements of NIH in order to ensure successful system integration of any new enhancements. The Contractor shall also provide personnel proficient in Oracle to identify system gaps, make recommendations and coordinate fixes as needed.

The contractor shall help the NIH implement administrative improvements and workflow automation establishing an agile IT platform that is scalable to meet the needs of large organizations, highly-distributed business operations, and diverse user communities. The team will take an enterprise approach including clearly understanding the broad business drivers and strategic vision of the organization as part of defining technical requirements and assessing appropriate tools and technologies to support workflow automation and organizational change. From this vantage point, they will assist the NIH in deploying the most appropriate technology solution(s) that: 1) establishes a digitized process development platform that supports workflow design and enhancements; 2) provides business intelligence and performance metrics for effective decision-making; and 3) integrates with existing (and future) IT investments across the enterprise.

NOTE: ALL SERVICES IN THIS TASK AREA ARE TO BE USED ONLY IN DIRECT SUPPORT OF THE OTHER TASK AREAS.

3.7 Task Area 7: Center of Excellence (CoE) Support

The COEs will provide agencies/Operating Divisions with consulting and engineering services to radically improve the way in which agencies design services and interact with the customers they serve, with a constant focus on meaningfully improving outcomes.

The COEs will work with customer agencies directly to identify their needs, recommend a solution, identify the best contract vehicle to procure support, and oversee implementation of the solution.

The COEs will work with customer agencies directly to identify their needs, recommend a solution, and oversee implementation of the solution.

Below are the Scope Descriptions for each of the CoEs:

a) Cloud Adoption Center of Excellence

Objective: Historically, agencies have experienced security, acquisition and complexity as barriers to adopting commercial cloud services. However, with the increased availability of FedRAMP certified providers, and acquisition vehicles for cloud services and skills, the CoE will seek to reduce subsequent barriers to agency cloud adoption. The Cloud Adoption Center of Excellence (Cloud CoE) will assist the

analysis of current systems and applications to provide recommendations for planning migration to the cloud, including balancing tactical “lift and shift” imperatives with more strategic “fix and shift” possibilities. By using an agile and flexible framework the CoE accelerate adoption across the executive branch enterprise.

Possible activities:

- Portfolio/Architecture Analysis
- Application/System Analysis
- Cloud Migration Planning
- Security Assessments and Innovations

b) IT Infrastructure Optimization Center of Excellence

Objective: The IT Infrastructure Optimization Center of Excellence will assist the strategic planning activities of federal agencies. This CoE will assist agencies develop a unified and optimized IT infrastructure, leveraging federally owned data centers, cloud computing services, and commercial data centers (e.g. co-location). The objective is to ensure the targeted agency has an integrated cloud computing and data center consolidation and optimization strategy. CoE IT Infrastructure subject matter experts will bolster the targeted agency modernization planning processes, assist with initial gap analysis, application rationalization, data center inventory, consolidation planning support, and/or migration planning.

Possible activities:

- Agency architecture assessments and end-state planning
- Network Consolidation
- Application inventory and rationalization
- Data Center Planning (e.g. assess end-state power, cooling, space, connectivity readiness)
- Organizational change management specific to data center closure
- Assessment of cloud capabilities and functions intersecting IT infrastructure
- Developing frameworks to target end state of systems environment
- Data quality assessments
- Master Data Management Strategy
- Data migrations
- Data conversions
- Identity Access Assessments
- IT Security Reviews (both cyber and IT facility security)
- Test systems and processes
- Decommission of legacy systems

c) Customer Experience Center of Excellence

Objective: The customer experience transformation is to create experiences that meet or exceed

customer expectations. To be successful, assistance will be provided to support and help agencies design outstanding experiences and the ecosystem to deliver them, demonstrate the business value of customer experience as a discipline, and lead its adoption across the organization.

Possible activities:

- Facilitating multi stakeholder meetings to define meaningful outcomes, metrics that matter to decision makers and the public
- Deliver a customer experience transformation approach
- Deliver an approach to tackling high impact/high value projects
- Help create foundations to drive cultural and operational change
- Build a customer experience culture
- Service Design-the cross-channel experience
- Designing the ideal journey
- Performance and measuring the customer experience
- Evaluate and map cross functional customer journeys
- Change management and organizational alignment
- Identify CX initiatives that produce results
- Help design model to sustain CX transformation over the long-term

d) Contact Center - Center of Excellence

Objective: Contact Center CoE subject matter experts will assist agencies with defining their customer experience journey and overall vision. Existing contact center systems, processes, operations, data and technologies will be examined, and recommendations made on future optimization and modernization plans.

Possible activities:

- Contact Center Optimization
- Utilization of Robotic Process Automation (RPA) and Intelligent Systems
- Knowledge Management
- Quality Assurance
- Workforce Management
- Telephony
- Infrastructure
- Innovative technologies and solutions
- Continuous process improvement
- Omni-channel service design
- Workforce management
- Culture and agent empowerment
- Central ownership of issues, resolution & opportunities to improve
- Performance Management
- Best practices and playbooks

e) Service Delivery Analytics Center of Excellence

Objective: Modernization and transformation efforts are focused on meaningful impact, with ability to measure the resulting improvement of outcomes for citizens. This will instrument service delivery processes to institute and manage continuous improvement.

Possible activities:

- Facilitating multi stakeholder meetings to define meaningful outcomes, metrics that matter to decision makers and the public
- Process Flow Charting (service design blueprinting)
- Data Analysis
- Interactive Dashboards
- Continuous Process Improvement for Services Provided
- Integration and configuration of measurement instruments (within CRMs, contact centers, websites, paper processing, etc.)

3.8 Task Area 8: Human Resources (HR) Solutions

The contractor shall provide human resources (HR) support services that include modeling, forecasting, needs analysis, and succession planning.

A non-exhaustive list of examples of the type of work to be performed under this task area includes:

- a. Training and Development Services, including:
 - Employee Training Needs Assessment,
 - Technical and General Skills,
 - Knowledge Training,
 - Leadership and Supervisory Development Training,
 - Career Development,
 - Training Program Management Support.

- b. Human Capital Strategy Services, including:
 - Talent/Performance Management,
 - Workforce and Succession Planning,
 - Diversity and Work–Life Programs,
 - Knowledge/Competency Management,
 - HR Systems Design and Consultation,
 - Branding,
 - Recruitment,
 - Staffing,
 - Communications Strategies,
 - Employee Engagement,
 - Program Implementation Support

- c. Organizational Performance Improvement, including:
 - Change Management,
 - Strategic Planning and Alignment,
 - Organizational Assessment and Transformation,
 - Business Process Reengineering,
 - Data Analytics,
 - Data-driven Performance Reviews

ARTICLE C.2. TASK ORDER REPORTING REQUIREMENTS

All reports required herein shall be submitted in electronic format. In addition, one hardcopy of each report shall be submitted to the Task Order Contracting Officer (TO CO).

All electronic reports submitted shall be compliant with Section 508 of the Rehabilitation Act of 1973. Additional information about testing documents for Section 508 compliance, including guidance and specific checklists, by application, can be found at: <http://www.hhs.gov/web/508/index.html> under "Making Files Accessible."

All paper/hardcopy documents/reports submitted under this contract shall be printed or copied, double-sided, on at least 30 percent post-consumer fiber paper, whenever practicable, in accordance with FAR 4.302(b).

TECHNICAL REPORTS**1. Monthly Progress Report**

This report shall include a description of the activities during the reporting period, and the activities planned for the ensuing reporting period. The first reporting period consists of the first full month of performance plus any fractional part of the initial month. Thereafter, the reporting period shall consist of each calendar month.

The first report shall be due on/before the 5th calendar day after the first full month of the contract. Thereafter, reports shall be due on or before the tbd Calendar day following each reporting period.

2. Weekly Progress Reports

This report shall include a description of the activities during the reporting period, and the activities planned for the ensuing reporting period. The first reporting period consists of the first full week of performance plus any fractional part of the initial week. Thereafter, the reporting period shall consist of each calendar week.

The first report shall be due on/before the 5th calendar day after the first full week of the contract. Thereafter, reports shall be due on or before the 5 day following each reporting period.

3. Quarterly Progress Report

a. This report shall include a [summation of the monthly progress reports/a description of the activities during the reporting period] and the activities planned for the ensuing reporting period. The first reporting period consists of the first full three months of performance including any fractional part of the initial month. Thereafter, the reporting period shall consist of three full calendar months.

b. A monthly report will not be submitted for the final month of the quarter.

c. The first report shall be due TBD per Task Order. Thereafter, reports shall be due on or before the TBD Calendar day following each reporting period.

4. Semi-Annual Progress Report

a. This report shall include a [summation of previously submitted monthly and/or

quarterly reports/a description of the activities during the reporting period] and the activities planned for the ensuing reporting period. The initial report will be submitted for the first full six months of the contract performance including any fractional part of the initial month. Thereafter, the reporting period shall consist of six full calendar months.

- b. Monthly and/or quarterly reports will not be submitted the month the semi-annual report is due.
- c. The first report shall be due TBD per Task Order. Thereafter, reports shall be due on or before the TBD Calendar day following each reporting period.

5. Annual Progress Report

This report shall include a summation of the results of the entire contract work for the period covered. An annual report will not be required for the period when the Final Report is due. A Monthly Report shall not be submitted when an Annual Report is due.

The first report shall cover the period TBD per Task Order through TBD per Task Order of this contract and shall be due [on TBD per Task Order/within 30 days after the Anniversary Date of the Contract.] Thereafter, reports shall be due on or before the TBD Calendar day following the reporting period.

The Contractor shall provide the Contracting Officer with TBD copies of the Annual Progress Report in draft form [in accordance with the DELIVERIES Article in SECTION F of this Contract/ TBD Calendar days prior to the delivery date for the Final Version of the Annual Report.] The Contracting Officer's Representative (COR) will review the draft report and provide the Contracting Officer with comments within TBD Calendar days after receipt. The Annual Progress Report shall be corrected by the Contractor, if necessary and the final version delivered as specified in the above paragraph.

6. Final Report

This report shall consist of the work performed and results obtained for the entire contract period of performance as stated in SECTION F of this contract. This report shall be in sufficient detail to describe comprehensively the results achieved. The Final Report shall be submitted on or before the last day of the contract performance period. A/An Annual report shall not be required for the period when the Final Report is due.

a. Other Reports/Deliverables

1. Source Code and Object Code

Unless otherwise specified herein, the Contractor shall deliver to the Government, upon the expiration date of the contract, all source code and object code developed, modified, and/or enhanced under this contract.

2. Information Security and Physical Access Reporting Requirements

The Contractor shall submit the following reports as required by the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract. Note: Each report listed below includes a reference to the appropriate subparagraph of this article.

a. Roster of Employees Requiring Suitability Investigations

The Contractor shall submit a roster, by name, position, e-mail address, phone number and responsibility, of all staff (including subcontractor staff) working under the contract who will develop, have the ability to access, or host and/or maintain a Federal information system(s). The roster shall be submitted to the Contracting Officer's Representative (COR), with a copy to the Contracting Officer, within 14 calendar days of the effective date of the contract. (Reference subparagraph A.e. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

b. IT Security Plan (IT-SP)

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the contractor shall submit the IT-SP within thirty (30) days after contract award. The IT-SP shall be consistent with, and further detail the approach to, IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The IT-SP shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of IT resources that are developed, processed, or used under this contract. If the IT-SP only applies to a portion of the contract, the Contractor shall specify those parts of the contract to which the IT-SP applies.

The Contractor shall review and update the IT-SP in accordance with NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, on an annual basis.

(Reference subparagraph D.c.1. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

c. IT Risk Assessment (IT-RA)

In accordance with HHSAR Clause 352.239-72, Security Requirements for Federal Information Technology Resources, the contractor shall submit the IT-RA within thirty (30) days after contract award. The IT-RA shall be consistent, in form and content, with NIST SP 800-30, Risk Management Guide for Information Technology Systems, and any additions or augmentations described in the HHS-OCIO Information Systems Security and Privacy Policy.

The Contractor shall update the IT-RA on an annual basis.

(Reference subparagraph D.c.2. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

d. FIPS 199 Assessment

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the Contractor shall submit a FIPS 199 Assessment within thirty (30) days after contract award. The FIPS 199 Assessment shall be consistent with the cited NIST standard.

(Reference subparagraph D.c.3. of the INFORMATION AND PHYSICAL ACCESS

SECURITY Article in SECTION H of this contract.

e. IT Security Certification and Accreditation (IT-SC&A)

In accordance with HHSAR Clause 352.239-72, Security Requirements For Federal Information Technology Resources, the Contractor shall submit written proof to the Contracting Officer that an IT-SC&A was performed within three (3) months after contract award.

The Contractor shall perform an annual security control assessment and provide to the Contracting Officer verification that the IT-SC&A remains valid.

(Reference subparagraph D.c.4. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

f. Reporting of New and Departing Employees

The Contractor shall notify the Contracting Officer's Representative (COR) and Contracting Officer within five working days of staffing changes for positions that require suitability determinations as follows:

- a. New Employees who have or will have access to HHS Information systems or data: Provide the name, position title, e-mail address, and phone number of the new employee. Provide the name, position title and suitability level held by the former incumbent. If the employee is filling a new position, provide a description of the position and the Government will determine the appropriate security level.
- b. Departing Employees: 1) Provide the name, position title, and security clearance level held by or pending for the individual; and 2) Perform and document the actions identified in the "Employee Separation Checklist", attached in Section J, ATTACHMENTS of this contract, when a Contractor/Subcontractor employee terminates work under this contract. All documentation shall be made available to the COR and/or Contracting Officer upon request.

(Reference subparagraph E.2.a-c. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

- g. Contractor - Employee Non-Disclosure Agreement(s)** The contractor shall complete and submit a signed and witnessed "Commitment to Protect Non-Public Information - Contractor Agreement" form for each contractor and subcontractor employee who may have access to non-public Department information under this contract. This form is located at: <https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf>.

(Reference subparagraph E.3.d. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

h. Vulnerability Scanning Reports

The Contractor shall report the results of the required monthly special vulnerability scans no later than 10 days following the end of each reporting period. If required monthly, this report may be included as part of the Technical Progress Report. Otherwise, this report shall be submitted under separate cover on a monthly basis.

(Reference subparagraph E.5. of the INFORMATION AND PHYSICAL ACCESS SECURITY Article in SECTION H of this contract.)

3. Section 508 Annual Report

The contractor shall submit an annual Section 508 report in accordance with the schedule set forth in the ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY Article in SECTION H of this contract. The Section 508 Report Template and Instructions for completing the report are available at: <http://www.hhs.gov/web/508/contracting/technology/vendors.html> under "Vendor Information and Documents."

Appendix A – Task Order Labor Category Descriptions and Requirements**1. PROJECT MANAGER**

Functional Responsibility: Manages multiple projects and project managers. Serves as the overall lead or director on complex projects and multiple agency contracts and serves as the principal liaison between the contractor and multiple government agencies. The Project Manager is responsible for ensuring that all tasking associated with a Government-funded program or project is completed effectively and efficiently, on time. Manages associated technical project issues. Assures quality control programs are in place and consistent on all programs assigned.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 5 years of relevant experience*

2. ASSISTANT PROJECT MANAGER

Functional Responsibility: Serves as a lead on complex projects and multiple agency contracts and serves as the principal liaison between the contractor and multiple government agencies. The Project Manager is responsible for ensuring that all tasking associated with a Government-funded program or project is completed effectively and efficiently, on time. Coordinates manpower and resources for multiple projects. Manages associated technical project issues. Assures quality control programs are in place and consistent on all programs assigned.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

3. ADMINISTRATIVE ASSISTANT

Functional Responsibility: In direct support of professional positions, conducts a variety of clerical and administrative activities. Maintains office files, provides word processing, spread sheets and graphics as desired; other duties as assigned.

Education: High school degree

Experience: No less than 1 to 2 years of relevant experience*

4. WEB PROJECT MANAGER

Functional Responsibility: Responsible for web strategy and operations. Develops business plan and annual budget for website function. Accountable for budget, staff planning, management, and products and service delivery. Oversees operational activities of the website(s) with specific attention aimed at content creation and website maintenance.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 3 years of relevant experience*

5. WEB DESIGNER

Functional Responsibility: Under general supervision, designs and develops user interface features, site animation, and special-effects elements. Contributes to the design group's efforts to enhance the look and feel of the organization's online offerings. Designs the website to support the organization's strategies and goals relative to external communications. . Develops applications based on current, new and future net-based applications. Requires significant graphics and design experience as well as HTML knowledge.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

6. WEB SOFTWARE DEVELOPER

Functional Responsibility: Experienced in the design and development, testing, deployment, and maintenance of web or web applications constructed in a business application or survey application mode. Experienced in developing 508 - compliant web applications for relational database and/or data retrieval systems.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

7. WEB CONTENT ADMINISTRATOR

Functional Responsibility: Responsible for developing and providing content that will motivate and entertain users so that they regularly access the website and utilize it as a major source for information and decision-making. Responsible for managing/performing website editorial activities including gathering and researching information that enhances the value of the site. Locates, negotiates, and pursues content. Seeks out customers to gather feedback for website improvement and enhancements. Requires experience in production management, web page design, HTML, and web graphics types and standards.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

8. BUDGET ANALYST

Functional Responsibility: Work with program and project managers to develop the organization's budget. Review budget proposals for completeness, accuracy, and compliance with laws and other regulations. Explain their recommendations for funding requests to other organization, legislators, and the public. Analyze proposed plans and find alternatives if the projected results are unsatisfactory. Monitor organizational spending to ensure that it is within budget. Inform program managers of the status and availability of funds. Estimate future financial needs.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

9. ACCOUNTING ANALYST

Functional Responsibility: Evaluates public company financial statements. Public companies issue (10-k) annual financial statements as required by the Security and Exchange Commission. The statements include the balance sheet, the income statement, the statement of cash flows and the notes to the financial statements. Specifically, the notes to the financial statements contain considerable quantitative detail supporting the financial statements along with narrative information.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

In addition, the analyst will most likely hold the Chartered Certified Accountant (ACCA) or Certified Public Accountant (CPA) or Chartered Account (CA or ACA) description

Experience: Has extensive training in understanding financial accounting principles for public companies based on generally accepted accounting principles as provided by the Financial Accounting Standards Board. Or, he/she may have additional experience in applying international accounting standards based on the rules put out by the International Accounting Standards Board

10. FINANCIAL MANAGER

Functional Responsibility: Responsible for the financial health of an organization. They produce financial reports, direct investment activities. And develop strategies and plans for the long term financial goals of their organization. Prepare financial statements, business activity reports, and forecasts. Monitor financial details to ensure the legal requirements are met. Supervise employees who do financial reporting and budgeting. Review company financial reports and seek ways to reduce costs. Help management make financial decisions.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 3 years of relevant experience*

11. PROCUREMENT SPECIALIST

Functional Responsibility: Ensures that the items and services to build and maintain advanced technology products are purchased from specified suppliers and are delivered according to agreed terms and conditions. An important aspect of this role is seeking maximum value for the company through time and cost agreements while working with technology advanced products. Reviews planned orders, creates requisitions for purchased items, and manage approval process. Tracks order acknowledgement, prepares and communicates shortage and backlog reports, and provides visibility of potential interruptions to internal customers. Reviews, updates, and maintains purchase orders until they are closed.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

12. SUBJECT MATTER EXPERT

Functional Responsibility: Experience in utilizing new methodologies for solving problems and ensuring that systems are in compliance with organizational requirements. Analyzes user needs to determine functional requirements, performs functional allocation to identify required tasks and their interrelationships. Develops recommendations for the organizational process changes to include new technology, identifies resources required for each task.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 5 years of relevant experience*

13. LOGISTICAL/TECHNICAL SUPPORT SPECIALIST

Functional Responsibility: Performs logistics tasks associated with logistics engineering, scientific or general data processing functions within Governmental and/or civil development. Acquisition, sustainment and/or operational environments, interfaces with individual users to resolve operational and/or business processes, and/or routine technical, problems. Coordinates tasks with other employees, trains and assists less-experienced personnel. Participates as individual contributor and as member of multiple cross functional integrated product teams and/or functional area teams.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

14. FUNCTIONAL SPECIALIST

Functional Responsibility: A functional specialist is an expert in a specific discipline, such as human resources, finance, marketing, information technology or continuous improvement. A specialist can either manage a department or take a key role in one area of the department. For example, a marketing specialist might oversee the research, distribution, sales, advertising, promotions, social media or public relations of a small business. At a large company, she might specialize by handling one of those duties. A specialist might not be able to handle all of the tasks in her area, but knows enough about them to manage others. For example, an advertising specialist will be familiar with media buying, layout and design, pay-per-click strategies and copywriting. While she might not have advanced layout and design skills, she understands the basics of graphic design and can direct a graphic artist. Respond to queries from students on the particular subject.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

15. SUBJECT MATTER EXPERT INSTRUCTOR

Functional Responsibility: Experienced practitioners that can develop and/or teach in a stimulating and participative learning environment for students. Work with other team members, such as Programmers, Graphic Designers, Writers, and Instructional Designers in order to produce effective learning modules in context with the implementation of self-learning methodologies. Develop model exam questions, including solutions and explanations. Create interactive exercises and activities to support learning outcomes.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: Not less than 5 years of relevant experience*

16. BUSINESS PROCESS REENGINEERING SPECIALIST

Functional Responsibility: Applies business process improvement practices to reengineer methodologies, principles, and business process modernization projects.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

17. SOFTWARE ARCHITECT

Functional Responsibility: Designs and develops new software products or major enhancements to existing software. Addresses problems of system integration compatibility, and multiple platforms. Responsible for project completion. Performs feasibility analysis on potential future projects to management

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

18. BUSINESS OPERATIONS SPECIALIST

Functional Responsibility: Addresses organizational sustainability issues, such as resource assessment, planning, and allocation; operations and work stream management; business continuity and disaster recovery strategies and solutions, including risk assessments, business impact analyses, strategy selection, and documentation of business continuity and disaster recovery procedures.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

19. HUMAN RESOURCES ANALYST

Functional Responsibility: Advises on the assessment, planning, and coordination of human resources activities of an organization. Activities may include policy planning, training and development, and organizational development and analysis. May work with management to organize the work setting to improve worker productivity. Conduct research studies of work environments, organizational structures, communication systems, morale and motivation to assess organizational functioning.

Education: MA/MS desired; a minimum of a Bachelor's Degree in relevant area.

Experience: No less than 1 to 2 years of relevant experience*

***NOTE: SUBSTITUTION OF EDUCATION FOR SPECIALIZED EXPERIENCE**

- Two full academic years of progressively higher level graduate education, masters, graduate, or professional degree may be substituted for one year of relevant experience.
- Fours additional years of relevant experience may be substituted for a Bachelor's Degree.