


| | | | | | | | | | | | | | | | |
|---|--|--|-----------------------------|--|-----------------------|--|---|---|--|--|----------------|--|------------|--|--|
| SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30 | | | | | 1. REQUISITION NUMBER | | PAGE 1 OF 77 | | | | | | | | |
| 2. CONTRACT NO. | | | 3. AWARD/ EFFECTIVE DATE | | 4. ORDER NUMBER | | | 5. SOLICITATION NUMBER 70FA4023R000000006 | | 6. SOLICITATION ISSUE DATE 03/09/2023 | | | | | |
| 7. FOR SOLICITATION INFORMATION CALL:  | | | a. NAME Janine Queen | | | b. TELEPHONE NUMBER (No collect calls) | | | 8. OFFER DUE DATE/LOCAL TIME 04/07/2023 1100 ET | | | | | | |
| 9. ISSUED BY FEMA-SUPPORT SERVICES SECTION FEDERAL EMERGENCY MANAGEMENT AGENCY 500 C STREET SW 3RD FLOOR WASHINGTON DC 20472 | | | | | CODE 70FA40 | | 10. THIS ACQUISITION IS <input type="checkbox"/> UNRESTRICTED OR <input checked="" type="checkbox"/> SET ASIDE: 100.00 % FOR: <input type="checkbox"/> SMALL BUSINESS <input checked="" type="checkbox"/> WOMEN-OWNED SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input checked="" type="checkbox"/> (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB NAICS: 541211 <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A) SIZE STANDARD: \$23.5 | | | | | | | | |
| 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 FEMA HEADQUARTERS 500 C STREET SW WASHINGTON DC 20472 | | | CODE FEMA/HQ | | | 16. ADMINISTERED BY FEMA-SUPPORT SERVICES SECTION FEDERAL EMERGENCY MANAGEMENT AGENCY 500 C STREET SW 3RD FLOOR WASHINGTON DC 20472 | | | CODE 70FA40 | | | | | | |
| 17a. CONTRACTOR/ OFFEROR | | | CODE | | | FACILITY CODE | | | 18a. PAYMENT WILL BE MADE BY | | | CODE | | | |
| TELEPHONE NO. | | | | | | | | | | | | <input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER | | 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM | |
| 19. ITEM NO. | | 20. SCHEDULE OF SUPPLIES/SERVICES | | | | | 21. QUANTITY | | 22. UNIT | | 23. UNIT PRICE | | 24. AMOUNT | | |
| 0001 | | The purpose of this procurement is to procure financial audit remediation support of internal controls and audit findings. The resulting Blanket Purchase Agreement (BPA) will be hybrid BPA that Firm-Fixed Price (FFP) and/or Labor Hour (LH) call orders will be able to be released against. Period of Performance: 06/16/2023 to 06/15/2028 Office of Chief Financial Officer Remediation Continued ... (Use Reverse and/or Attach Additional Sheets as Necessary) | | | | | 1 | | LO | | | | | | |
| 25. ACCOUNTING AND APPROPRIATION DATA | | | | | | | | | | 26. TOTAL AWARD AMOUNT (For Govt. Use Only) | | | | | |
| <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) Shawn Smith | | | | 31c. DATE SIGNED | | | |

| 19. ITEM NO. | 20. SCHEDULE OF SUPPLIES/SERVICES | 21. QUANTITY | 22. UNIT | 23. UNIT PRICE | 24. AMOUNT |
|-----------------|--|-----------------|-------------|-------------------|---------------|
| 0002 | Support Labor FFP Labor - Remediation Support Services Firm-Fixed Price: Definite Goal or Target Specifying End Product Price will be determined at the Call Order Level Product/Service Code: R704 Product/Service Description: SUPPORT- MANAGEMENT: AUDITING Office of Chief Financial Officer Remediation Support Labor LH (NTE) Labor - Remediation Support Services Labour Hours (Not to Exceed): Definite Goal or Target Specifying End Product Price will be determined at the Call Order Level Product/Service Code: R704 Product/Service Description: SUPPORT- MANAGEMENT: AUDITING | 1 | LO | | |

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

| | | | | |
|---|------------------------|------------------------------------|---|-----------------------|
| 32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | | 32c. DATE | 32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE | |
| 32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE | | | 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE | |
| | | | 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE | |
| 33. SHIP NUMBER | 34. VOUCHER NUMBER | 35. AMOUNT VERIFIED CORRECT FOR | 36. PAYMENT | 37. CHECK NUMBER |
| <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL | | | <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL | |
| 38. S/R ACCOUNT NUMBER | 39. S/R VOUCHER NUMBER | 40. PAID BY | | |
| 41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT | | | 42a. RECEIVED BY (<i>Print</i>) | |
| 41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER | | 41c. DATE | 42b. RECEIVED AT (<i>Location</i>) | |
| | | | 42c. DATE REC'D (YY/MM/DD) | 42d. TOTAL CONTAINERS |

| | |
|--|----|
| A - Solicitation/Contract Form..... | 3 |
| B - Supplies or Services/Prices..... | 3 |
| C - Description/Specifications..... | 4 |
| D - Packaging and Marking..... | 22 |
| E - Inspection and Acceptance | 22 |
| F - Deliveries or Performance | 23 |
| G - Contract Administration Data | 24 |
| H - Special Contract Requirements | 26 |
| I - Contract Clauses | 46 |
| J - List of Documents, Exhibits and Other Attachments | 60 |
| K - Representations, Certifications, and Other Statements of Bidders | 60 |
| L - Instructions, Conditions, and Notices to Bidders | 65 |
| M - Evaluation Factors for Award..... | 74 |

A - Solicitation/Contract Form

B - Supplies or Services/Prices

CONTRACT (BPA CALL) TYPE

B.1 CONTRACT TYPE

This is a Blanket Purchase Agreement (BPA) with multiple price structures available to the government – Firm-Fixed-Price and/or Labor Hour – which will be identified during Request for Proposal.

The period of performance for this Agreement will be for one (1) year with four (4) option years in accordance with FAR 8.405-3(d)(2), because this will be a single-award BPA.

Call orders will be awarded in accordance with the call order procedures stated in Section H. Call orders awarded under the BPA Agreement may be Firm-Fixed-Price or Labor Hour only.

Call orders may be issued for up to one (1) year with four (4) option years. Call orders may be issued up until the last day of the BPA's period of performance. More targeted call orders may be issued for periods of less than one year also.

B.2 DATA

Data will be required for all call orders and shall be priced within the effort proposed as Labor and shall not be separately priced.

B.3 CONTRACT MIN/MAX AMOUNT

There are no Minimums or Maximums associated with the BPA for the FEMA Wide Strategic Sourcing Vehicle for Office of Chief Financial Officer (OCFO) Financial Management Division (FMD) Remediation Support Services requirement.

B.4 PROGRAM CEILING

There is no ceiling value associated with this BPA; however, if the cumulative (or estimated) value of all call orders released against this single-award BPA, approvals to exceed this amount will need to obtain approvals in accordance with FAR 8.405-3(a)(3)(ii).

B.5 LABOR CATEGORIES

B.5.1 The BPA is for a base year and four option years and the below individual rates are the rates that can be charged for each of the five years. The labor categories and pricing rates are to be proposed in the Section J attachment below table:

| HOURLY RATES PROPOSED BY YEAR | | | | | |
|-------------------------------|-----------|--------|--------|--------|--------|
| Direct Labor Categories | Base Year | Year 1 | Year 2 | Year 3 | Year 4 |
| Sr. IT Security Consultant | | | | | |
| IT Specialist | | | | | |
| Senior Management | | | | | |
| Audit Sr. Management III | | | | | |
| Audit Lead III | | | | | |
| Staff II | | | | | |
| Senior Manager | | | | | |
| Manager | | | | | |
| Audit Sr. Project Support III | | | | | |
| Audit Project Support - V | | | | | |

B.5.2 The estimated hours per labor category can be found in the pricing template in Section J.

B.6 CONTRACTING OFFICER'S AUTHORIZED TO ORDER

All Federal Emergency Management Agency (FEMA) Headquarters Contracting Officers may issue call orders against this call order. Once a call order is issued, provide the BPA Contracting Officer a copy of the call order for value tracking purposes only.

C - Description/Specifications

PERFORMANCE WORK STATEMENT (PWS)

Office of Chief Financial Officer (OCFO)
Risk Management and Compliance Division
Remediation Support of Internal Controls and Audit Findings

PART 1

General Information

1.0 General: This is a non-personnel services contract to provide contractor support for internal controls and financial audit remediation services for the Office of the Chief Financial Officer (OCFO), Risk Management and Compliance Division (RMC). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction: The Contractor shall provide non-personal services necessary to perform financial audit remediation support of internal controls and audit findings. The Contractor shall provide all personnel, supplies, transportation, tools, materials, supervision, and other items necessary to perform the required services except those items specified as government furnished property and services. The Contractor shall perform to the standards in this contract.

1.2 Background: The Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), OCFO requires Contractor support services with expertise in federal government auditing functions. The mission of the RMC Division is to direct the Branch's resources towards ensuring accuracy and completeness in financial data by producing reliable information, safeguarding assets, and effectively detecting and responding to errors, fraud, or theft in accordance with DHS policies and Federal laws.

1.3 Objectives: The service objective is to provide support for financial audit remediation of internal controls and audit findings to meet all [GAO Green Book](#), [OMB A-123](#), and DHS and FEMA requirements.

1.4 Scope: FEMA requires Contractor support for audit remediation support services with knowledge and expertise of federal government requirements in the following functional areas to support FEMA's compliance to:

- DHS Financial Accountability Act (FAA)
- Chief Financial Officers' Act (CFO)
- Federal Financial Management Improvement Act (FFMIA)
- Federal Managers Financial Integrity Act (FMFIA)
- Office of Management and Budget Circular A-123, "Management's Responsibility for Internal Control;"
- Payment Integrity Information Act of 2019, Public Law 116-11 (PIIA)
- National Institute of Standards and Technology (NIST) Special Publication 800-53
- Federal Information System Control Audit Manual (FISCAM)
- Other relevant policy guidance, laws, and regulations governing financial internal controls including IT internal controls requirements for the FEMA

Work efforts include remediation support of internal controls and audit findings in the following categories:

- Execution, assessment, and monitoring of all aspects of OMB Circular A-123
- Enterprise and program planning
- Business Process Reengineering
- Cybersecurity
- Flood Insurance Operations Management
- Grants Management
- Data Analytics
- Human Capital Management
- Program integration to support both the Program Offices and OCFO in improving and remediating the overall control environment.
- Information Technology Systems
- Property

Contractors must be available to supplement current FEMA staff at length through the entire fiscal year and have the expertise of federal government financial and accounting requirements in order to remediate internal controls and audit findings. The Contractor shall:

- Remediate business process findings to ensure compliance with GAO Green Book Standards
- Document remediation efforts to ensure compliance with GAO Green Book Standards
- Test remediation efforts to validate compliance with GAO Green Book Standards.
- Remediate IT control findings and related risks to ensure compliance with GAO Green Book Standards.

This may require contractors to travel to where disaster work is required for a temporary time (e.g., 2 weeks at a time with approval from the COR/CO).

1. Period of Performance: The period of performance shall be for five (5) year order period beginning from date of award.

1.6 General Information

1.6.1 Quality Control: The Contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The Contractor shall develop and implement

procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's quality control program is the means by which it assures the work completed complies with the requirements of the contract. The quality control program shall be delivered to the Contracting Officer's Representative (COR) within 15 days after contract award. Thereafter quality and risk related discussions will be a part of the Monthly Status Report. After acceptance of the quality control plan, the Contractor shall receive the Contracting Officer's acceptance in writing of any proposed change to his QC system.

1.6.2 Quality Assurance: The Government shall evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure that the Contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.6.3 Recognized Holidays: The Contractor is not required to perform work on the Government holidays listed below.

| | |
|-----------------------------------|------------------|
| New Year's Day | Labor Day |
| Martin Luther King Jr.'s Birthday | Columbus Day |
| President's Day | Veteran's Day |
| Memorial Day | Thanksgiving Day |
| Juneteenth | Christmas Day |
| Independence Day | |

1.6.4 Security Requirements: Contractor personnel performing work under this contract will be required to have a background investigation. A favorably adjudicated background is necessary throughout the life of the contract.

Physical Security: The Contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.4.1 Security Training: All personnel require access to information up to the sensitive but unclassified, for official use only (FOUO) levels. Contractor must ensure Contractor employees receive a favorably adjudicated public trust suitability prior to entry on duty (EOD). All individuals will be U.S. citizens. The Contractor shall follow the standards established within DHS and FEMA policy.

1.6.4.2 Certificate of Training: Certificate of training is required for all cleared contractor employees who are working with classified or unclassified information. All certificates must be sent to the assigned FEMA COR, before the Contractor or subcontractor is granted access to classified or unclassified information but no later than 30 calendar days after awarded contract. Send certificates of completion for Unauthorized Disclosure, OPSEC, and Insider Threat to the FEMA COR no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

1.6.4.2.1 Unauthorized Disclosure of Classified or Unclassified Information: Contractors and subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training. Access to the training can be obtained at:
<https://securityawareness.usalearning.gov/disclosure/index.html>

1.6.4.2.2 OPSEC Training: Contractors and subcontractors who are working on this contract shall receive the OPSEC Awareness Brief. Access to the briefing can be obtained at
<https://securityawareness.usalearning.gov/opsec/>

1.6.4.2.3 Insider Threat Training: Insider Threat training for contractors can be found at:
<https://securityawareness.usalearning.gov/itawareness/index.htm#>

1.6.4.3 For Official Use Only (FOUO) Information

1.6.4.3.1 In accordance with DHS Management Directive 11042.1 contractors, consultants and others to

whom access is granted will abide by 11042.1; DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

1.6.4.3.1.1 The contractor shall:

1.6.4.3.1.2 Be aware of and comply with the safeguarding requirements for “For Official Use Only” (FOUO) information as outlined in this directive.

1.6.4.3.1.3 Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.

1.6.4.3.1.4 Be aware that divulging information without proper authority could result in administrative or disciplinary action.

1.6.4.4 Contractors and consultants shall execute a DHS Form 11000-6, Sensitive but Unclassified Information Non Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon date of the DHS Policy and not applied retroactively.

1.6.5 Special Qualifications: The Contractor is responsible for ensuring at least one employee who is working on SharePoint has FEMA SharePoint certification available via the Office of the Chief Information Officer (OCIO).

1.6.6 Post Award Conference/Progress Meetings: In accordance with the Federal Acquisition Regulation (FAR) Subpart 42.5, the Contractor shall attend a post award conference convened by the contracting activity or contract administration office no later than five (5) business days after award.

The Contracting Officer, COR, and other Government personnel, as appropriate, may conduct progress meeting periodically with the Contractor to review the contractor’s performance. At these meetings the Contracting Officer will apprise the Contractor of how the government views the Contractor’s performance and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.7 Contracting Officer Representative (COR): The COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor’s performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially regarding changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract vehicle.

1.6.8 Key Personnel: The following personnel are considered key personnel by the government: Senior Information Security Consultant, Senior Manager, Audit Senior Management III, and Audit Lead III. Prior to replacing any of these personnel the Contractor will submit a resume on the perspective replacement to obtain CO or COR approval of the perspective replacement contractor within fifteen (15) days of notification of a vacancy. Once approval is received, the Contractor has three (3) days to submit security paperwork. If an alternate Contractor personnel is used temporary (no more than thirty (30) days) prior to the approved key personnel onboarding, the alternate must also receive approval from the CO or COR prior

to commencing work. For non-key personnel, replacements must be replaced and working on this contract no later than thirty (30) calendar days of the prior individual leaving. If the security process prevents this, additional time may be granted by the CO or COR.

The Contractor shall provide a Contract Manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the manager is absent shall be designated in writing to the Contracting Officer. The contract manager or alternate shall have full authority to act for the Contractor on all contract matters relating to daily operation of this contract. The Contract Manager or alternate shall be available between 9:00am-5:30pm, Monday thru Friday except Federal holidays or when the Government facility is closed for administrative reasons.

1.6.9 Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed. Ability to obtain a FEMA badge is required. It is also required for the Contractor to display the badge while at FEMA Headquarters.

1.6.10 Contractor Travel: Travel may be required to support this requirement to the Winchester, Virginia office or to the Regional field locations within the Continental United States (CONUS), including potential disaster sites. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor will not be reimbursed for local travel in the Washington, D.C. metropolitan area. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

1.6.11 Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.6.12 Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.13 Phase In/Phase Out Period: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the thirty (30) day phase in/ phase out periods. The Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

1.6.14 Hours of Operation: The Contractor is responsible for conducting business, between the hours of 9:00 am – 5:30 pm Monday through Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. However, there may be occasions when Contractor employees shall be required to work other

than normal business hours, including weekends and holidays, to fulfill requirements under this PWS. For other than firm fixed price task orders under this contract, the Contractor will not be reimbursed when the Government facility is closed for the above reasons. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.15 Place of Performance: The work to be performed under this contract will be performed at both vendor facilities, via routine or episodic telework as agreed upon by program office, or at FEMA Headquarters—500 C Street SW, Washington, DC 20024. If the Contractor has a telework policy, they are required to submit a telework plan to the COR, PM and to the CO after contract approval. Any telework request must show how the Contractor will ensure full execution of the contract.

PART 2

Definitions & Acronyms

2.0 Definition and Acronyms

2.1 Definitions

2.1.1 **CONTRACTOR**. A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.

2.1.2 **CONTRACTING OFFICER**. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.

2.1.3 **CONTRACTING OFFICER'S REPRESENTATIVE (COR)**. An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4 **DEFECTIVE SERVICE**. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.5 **DELIVERABLE**. Anything that can be physically delivered but may include non-manufactured things such as meeting minutes or reports.

2.1.6 **KEY PERSONNEL**. Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the Key Personnel listed in the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.7 **PHYSICAL SECURITY**. Actions that prevent the loss or damage of Government property.

2.1.8 **QUALITY ASSURANCE**. The government procedures to verify that services being performed by

the Contractor are performed according to acceptable standards.

2.1.9 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.10 QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of a product or service shall meet contract requirements.

2.1.11 SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.13 WORKDAY. The number of hours per day the Contractor provides services in accordance with the contract.

2.1.14 WORK WEEK. Monday through Friday, unless specified otherwise.

2.2 Acronyms

| | |
|------------|--|
| CAP | Corrective Action Plans |
| CFO | Chief Financial Officer Act |
| CO | Contracting Officer |
| COR | Contracting Officer Representative |
| CPARS | Contractor Performance Assessment Reporting System |
| DHS | Department of Homeland Security |
| FAA | DHS Financial Accountability Act |
| FAR | Federal Acquisition Regulation |
| FEMA | Federal Emergency Management Agency |
| FFMIA | Federal Financial Management Improvement Act |
| FISCAM | Federal Information System Control Audit Manual |
| GAO | US Government Accountability Office |
| Green Book | Standards for Internal Control in the Federal Government |
| IPERA | Improper Payments Elimination and Recovery Act |
| IPIA | Improper Payments Information Act |
| IT | Information Technology |
| MAP | Mission Action Plans |
| NIST | National Institute of Standards and Technology |
| OA | Office of the Administrator |
| OMB | Office of Management and Budget |
| OCI | Organizational Conflict of Interest |
| OCFO | Office of the Chief Financial Officer |
| PIIA | Payment Integrity Information Act, 2019, Public Law 116-11 |
| POC | Point of Contact |
| PRS | Performance Requirements Summary |
| PWS | Performance Work Statement |
| QA | Quality Assurance |
| QAP | Quality Assurance Program |
| QASP | Quality Assurance Surveillance Plan |
| QC | Quality Control |
| QCP | Quality Control Program |
| RMC | Risk Management and Compliance Division |
| TOD | Test of Design |
| TOE | Test of Effectiveness |

PART 3

Government Furnished Property, Equipment, and Services

3.0 Government Furnished Property, Equipment, and Services

3.1 Services: The Government will facilitate SharePoint certification with the Office of the Chief Information Officer for those Contractor personnel that require it.

3.2 Facilities: For Contractor personnel working onsite at FEMA HQ, the Government will provide desk space, printers and other items necessary to maintain an office environment for Contractor personnel to conduct Government business.

3.3 Equipment: The Government will provide laptops and/or what the contractor will have access to, i.e., scanners, fax machines, printers, etc.

PART 4

Not Applicable. This page is left intentionally blank.

PART 5

Specific Tasks

5.0 Specific Tasks

5.1 Basic Services: The Contractor shall provide remediation of internal controls and audit findings for the OCFO RMC Division. Any time frame outside of the Acceptable Quality Level for any task is considered unacceptable, and may be reported in the Contractors Contractor Performance Assessment Reporting System (CPARS) report under the Schedule tab.

The following bullets provide a general overview of the required support under this contract and further details are described in Tasks One and Two in Sections 5.2 and 5.3 below:

- Assist the Government in the development of corrective action plans to resolve material weaknesses, significant deficiencies/reportable conditions, and control deficiencies that are identified by auditors, management, and other entities that satisfy the DHS Mission Action Plan Guide including the following topics: Control Deficiency Identification, Issue Description, Financial Statement and Management Control Assertions Mission Link, Root Causes, Key Strategies, Key Performance Measures, Resources Required, Verification and Validation, Risks and Impediments, Dependencies, Milestones, Critical Milestones with Due Dates and Status. Include incorporating lessons learned from prior assessments.
- Provide the Government with process improvement recommendations for internal controls over financial reporting, internal controls over operations and conformance with Federal Financial Management Systems Conformance.
- Provide the Government with process improvement recommendations for controls that support DATA Act reporting.
- Assist in remediating system controls and processes that support data quality and security, in accordance with the Federal Information System Controls Audit Manual (FISCAM), DHS 4300 A policy, and other applicable guides.
- Support the review and implementation of new requirements as issued through legislative acts, presidential orders, and/or other regulatory bodies.
- Provide expert technical advice and services, business processes and financial system internal control review support, and assistance in developing and implementing management processes.
- Develop and update, to include project plans, necessary tracking tools as-well-as formal and informal briefing documentation and presentations to ensure timely completion of internal control and financial audit remediation efforts.
- Prepare, for Government approval, educational resources; including, but not limited to— white papers, frequently asked questions (FAQs), resource guides, and standard operating procedures to support outreach efforts.
- User Training: The Contractor shall provide, for management and support of personnel, user training and guidance on all tools and methods developed in support of audit remediation and OCFO initiatives. This training shall include on-site and/or virtual training as well as written materials. User training includes the development of a training plan, training materials and conducting user training.

5.2 TASK ONE. Corrective Action Plans and Verification & Validation (V&V)

5.2.1 The Contractor shall provide direct support and assistance in the development, implementation, and maintenance of the Corrective Action Plan (CAP) or Mission Action Plan (MAP). The CAP/MAP will provide an overall blueprint for remediation plans and monitoring of weaknesses identified through internal and external reviews/audits. This task will include the development of reports, tools and templates to implement and monitor the plan and reflect the OCFO's communications and control tools. It will identify all key remediation elements, including the roles and responsibilities of key stakeholders, program objectives, program scope, milestones, and communication. Also, the Contractor shall assist in strategic planning and development, and provide programmatic advice on regulations that may have an impact upon CAP/MAP sustainment. For IT, CAP/MAPs are referred to as POA&Ms.

5.2.2 The CAP/MAP tasking will include support for developing Mission Action Plans (MAP) (DHS Deliverables which are similar to the FEMA CAP/MAP) to remediate control deficiencies identified within the Assurance Statement, annual Risk Assessment, OMB Circular A-123 Assessments, Independent Auditors report, and other relevant control deficiencies.

5.2.3 The Contractor shall also assist with V&V, which facilitates FEMA's remediation of control deficiencies to ensure that the fundamental issues are resolved, and progress is substantiated.

5.2.4 The execution of V&V shall include but is not limited to:

- Analyzing whether the project plans address the core issues and provide a viable basis to remediate the control deficiencies identified
- Reviewing completed milestones and discussing actions taken with the relevant process owners for the program offices under assessment
- Executing a customized Test of Design (TOD) to determine whether milestones and other work completed were designed and implemented to remediate deficiencies identified
- Executing a Test of Effectiveness (TOE) to evaluate whether the milestones and other work completed is executed as designed
- Concluding on the overall results of the TOD and TOE. The focus of the TOE assessment will be on re-performing key controls using statistical sampling where appropriate

5.2.5 Some of the key activities are facilitating root cause analysis, identifying key stakeholders, coordinating with respective process owners for the program offices under assessment to develop milestones, monitoring milestone progression, and assisting with the identification, mitigation and reporting of risk, which includes providing responses, if required. The Contractor shall also help identify critical path milestones for reporting to DHS, where necessary.

5.3 TASK TWO. Technical Assistance

The Contractor shall provide support in all areas of the major programs of FEMA related to internal controls, audit, and business process improvement for technical remediation and business process improvement.

5.3.1 Technical Remediation and Business Process Improvement:

1. The Contractor may be required to support follow-on taskings specifically related but not limited to remediation of identified risk areas and/or design and execution of control deficiencies identified through V&V and include updating or maintaining automated tools like SharePoint sites and analytic tools in Access. The Contractor will execute remediation in accordance with guidance issued by OMB, DHS, and OCFO.
2. The Contractor shall develop the remediation strategy with clearly defined out-puts and deliverables and provide a written weekly status report on contract execution to RMC. These efforts will be ongoing throughout the year.

PART 6

Contractor Personnel

6.0 CONTRACTOR PERSONNEL

6.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this PWS. Contractor staff shall have the below skill sets:

1. Knowledge in how to perform audits/assessments of internal controls over financial reporting and operations, IT, grants, insurance, and IT security in the Federal Government.
2. Knowledge in OMB and General Accounting Office (GAO) requirements and how to apply those requirements to complex internal control or assurance related projects throughout their entire life cycle and related phases including planning, assessing, testing, and reporting.
3. Knowledge in how to develop strategies for remediation of material weaknesses and other control deficiencies at the Federal level.
4. Experience in the development of policies and procedures, such as management directives, standard operating procedures, financial policies, tutorials, presentations, training materials, and workshops.
5. Experience presenting information about internal control topics in various settings including, but not limited to, small briefings involving high level management or executives, seminars, symposiums, one-on-one situations, etc.; and
6. Experience producing deliverables in alternate formats including, but not limited to, Word, Excel, Access, PowerPoint, and Visio.
7. Expert knowledge in federal accounting standards and the US Standard General Ledger (USSGL).
8. Expert knowledge of FISCAM, Federal Information Security Modernization Act (FISMA) and NIST.
9. Have knowledge of the OMB Circular A-123.

The table below details education, years of experience primary responsibility for key and non-key qualified Contractor personnel. There is no substitution for work experience in lieu of any required degrees.

| Labor Category | Primary Responsibility | Education | Certification | Years of Experience |
|---|--|-----------|---------------|---------------------|
| Senior Information Technology Security Consultant (KEY) | The Senior IT Security Consultant must have experience in the following areas: 1) development of target enterprise security architectures; 2) preparation for, readiness evaluation for, and assessment of IT systems and infrastructure certification and accreditation documentation and associated controls; 3) enterprise security program assessment; 4) compliance with FISMA requirements; 5) contingency management and disaster recovery; and 6) security education training and awareness. | Masters | CISA | 7 |

| | | | | |
|-----------------------------------|--|---------------------------|-----|----|
| Senior Manager (KEY) | Senior Managers, assisted by Managers and Audit Seniors, are responsible for daily management of the engagement including, but not limited to discussing audit findings with client/auditee personnel, drafting and reviewing audit reports, supervision of senior and junior auditors, periodic formal and informal status briefings to clients and developing audit programs, preparing status reports, and providing technical assistance on complex accounting and/or auditing issues. On non-financial audit assignments, the Senior Manager is similarly responsible for staff supervision, overall planning, and client contacts, assisted as necessary by subject matter experts, and may provide general business consulting services including research, reports, regulatory development assistance, and strategy formulation. | Bachelor's Degree (BA/BS) | CPA | 8 |
| Audit Senior Management III (KEY) | The Audit Senior Management provides top level management and technical review for the project management team, solves problems and leads Financial Statement & Internal Control Audit and Internal Audit Transformation engagements in conformity with generally accepted accounting principles. The Audit Senior Management communicates project status, concerns and updates to the client, providing quality control, alternative analytical approaches while keeping the timelines and funding on schedule. | Bachelor's Degree (BA/BS) | | 10 |
| Audit Lead III (KEY) | The Audit Lead provides strategic direction on financial statement and internal control audit, internal audit transformation and internal audit preparedness engagements. The Audit Lead oversees the team, developing, maintaining and monitoring the work plans, reviewing financial issues and providing direction on strategic matters and compliance. | Bachelor's Degree (BA/BS) | CPA | 8 |
| Information Technology Specialist | Assists the Project Director by providing specialized knowledge that helps plan the information systems portion of the engagement, including audit and SAS-70 engagements. Identifies appropriate information systems substantive testing, provides insight into potential information systems risks, and tests information systems security. The Information Technology Specialist may also lead audit teams in the actual performance of audit work for specific information systems. | Bachelor's Degree (BA/BS) | | 4 |
| Staff II | Staff II Accountants are responsible for performing auditing procedures including complex auditing procedures under the supervision of a Senior Accountant. Responsibility encompasses audit tests (both internal control and substantive), as well as | Bachelor's Degree (BA/BS) | | 1 |

| | | | | |
|----------------------------------|--|---------------------------|--|---|
| | vouching transactions, verifying, recalculating account balances, and account reconciliations. Staff II Accountants work under the supervision of a Senior Accountant or Manager. On non-audit assignments, Staff II similarly operate under supervision of Seniors or Managers, and may provide research, analysis, reporting, and evaluation support on business consulting engagements. | | | |
| Senior | Seniors are responsible for the supervision of Junior Staff, assisting in drafting reports and findings, addressing most accounting and auditing issues, execution of the more complicated procedures of the audit, writing planning memorandums, and developing audit sampling plans. On non-financial audit assignments, Seniors are similarly responsible for Junior Staff supervision, and may provide general business consulting services, including performing research, analysis, and reporting. | Bachelor's Degree (BA/BS) | | 2 |
| Manager | Managers, assisted by Audit Seniors, are responsible for daily management of the engagement including, but not limited to: discussing audit findings with client/auditee personnel, drafting and reviewing audit reports, supervision of senior and junior auditors, periodic formal and informal status briefings, developing audit programs, preparing status reports, and providing technical assistance on complex accounting and/or auditing issues. On non-financial audit assignments, the Manager is similarly responsible for staff supervision, overall planning, and client contacts, assisted as necessary by subject matter experts, and may provide general business development assistance, and strategy formulation. | Bachelor's Degree (BA/BS) | | 5 |
| Audit Senior Project Support III | The Audit Senior Project Support serves as the subject matter expert, instructing, directing, and monitoring the audit engagements on Financial Statement & Internal Control Audit and Internal Audit Transformation work. The Audit Senior Project Support provides senior management with analysis, status reports, recommendations and conclusions on the engagement progress. | Bachelor's Degree (BA/BS) | | 4 |
| Audit Project Support – V | The Audit Project Support conducts research, refines data, and assesses financial statements and reports on Financial Statement & Internal Control Audit and Internal Audit Transformation client engagements. The Audit Project Support assists senior management with process improvement diagnoses, financial modeling and documentation, and audit management. | Bachelor's Degree (BA/BS) | | 3 |

6.2 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the DHS. The Project Manager shall ensure Contractor employees understand and abide by DHS established rules, regulations and policies concerning safety and security.

6.3 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer or the COR), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

Part 7

Contractor Onsite Responsibilities

1. ONSITE CONTRACTOR FACILITY ACCESS

Federal employees, contractors, and visitors who enter a federal facility or site must follow facility signage and requirements, and agency safety protocols, regarding vaccination and testing documentation.

Note that there may be additional requirements for each facility and location with regards to masking and social distancing, hence it is important to adhere to the signage and protocols each location has in place to ensure a safe workspace.

7.1. COVID-19 Return to the Workplace Testing Protocols

FEMA requires all contractors and official visitors to follow all COVID-19 protocols. As of March 4, 2022, FEMA will maintain testing protocols at all facilities, regardless of the COVID-19 Community Level. Employees, contractors, and visitors who are not fully vaccinated to obtain a negative COVID-19 test result received within the past 24 hours prior to entering a FEMA facility or have proof of 90-day testing exemption following COVID-19 diagnosis and recovery.

The following procedures apply to this contract when entering a FEMA facility:

- Individuals are prohibited from entering FEMA controlled sites if they feel ill or are experiencing any COVID-19 symptoms.
- Onsite contractor employees and official visitors should be provided with the [Certification of Vaccination form](#) when they enter a FEMA facility.
- Contractors and official visitors who attest to being fully vaccinated on the Certificate of Vaccination form are exempt from testing requirements.
- FEMA will not maintain copies of the completed forms.
- Acceptable negative test results include pictures, screenshots, printouts, or medical documentation on official letterhead clearly indicating the name of the person, results of the test taken, the facilitator of the test, and date of testing. E-mailing or texting of this documentation is prohibited.
- Individual seeking entry into a FEMA facility who are not fully vaccinated will be offered a test kit free of charge.
- Contractors who refuse to participate in the entry testing or exemption as listed above will be denied entry and instructed to contact their supervisor and COR.

- Contractors have the authority to serve as a host/sponsor of a visitor, and thus, allow entry per these entry requirements.
- Upon visual verification of a visitor's documentation (Certificate of Vaccination form) for completeness or negative test result, allow entry to the site.

Part 8

Government Furnished Resources

1. GOVERNMENT FURNISHED RESOURCES

The Government will provide the workspace, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement.

Part 9

Government Acceptance Period

1. GOVERNMENT ACCEPTANCE PERIOD

The FEMA COR or the Project Manager will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the FEMA COR or Project Manager will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

9.1 The COR or the FEMA Project Manager will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

9.2 The COR or the FEMA Project Manager (PM) will have ten (10) business days to review deliverables and make comments. The Contractor shall have five (5) business days to make corrections and redeliver.

9.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

Part 10

Deliverables

10.0 DELIVERABLES

The Contractor shall submit the below deliverables for all efforts. Additional deliverables may be required on an as needed basis. All deliverables will undergo FEMA OCFO Management, Program process owner, COR and FEMA PM review

| ITEM | PWS REFERENCE | 1. DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|------|------------------|---------------------------|--------|--------------|
|------|------------------|---------------------------|--------|--------------|

| | | | | |
|---|-------|-----------------------|---|--|
| 1 | 1.6.6 | Post Award Conference | Five Business days after Contract Award | N/A |
| 2 | 1.6.6 | Progress Meeting | Periodically throughout the period of performance of contract | N/A |
| 2 | 11.0 | Progress Reports | Monthly within ten (10) business days after the end of each month | COR, Contracting Officer, FEMA Project Manager |

| ITEM | PWS REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|------|---------------|---|-------------------------------|-------------------------------|
| | | Corrective Action Plans and V&V | | |
| 1 | 5.2 | List of solicited Remediation Plans | Specified at Call Order level | Specified at Call Order level |
| 2 | 5.2 | Completed POA&Ms, Corrective Action Plan, and if applicable, DHS templates for Mission Action Plans | Specified at Call Order level | Specified at Call Order level |
| 3 | 5.2 | Plan reporting | Specified at Call Order level | Specified at Call Order level |
| 4 | 5.2 | Reporting of remaining risk and risk mitigation plans, and where applicable, whether compensating controls exist or | Specified at Call Order level | Specified at Call Order level |

| | | | | |
|--|--|-----|--|--|
| | | not | | |
|--|--|-----|--|--|

| ITEM | PWS REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|------|------------------|--|----------------------------------|----------------------------------|
| | | Technical Assistance | | |
| 1 | 5.3 | Risk Reduction recommendations | Specified at Call Order level | Specified at Call Order level |
| 2 | 5.3 | Executive briefings | Specified at Call Order level | Specified at Call Order level |
| 3 | 5.3 | Decision documents | Specified at Call Order level | Specified at Call Order level |
| 4 | 5.3 | Project Charters that contain, but are not limited to: <ul style="list-style-type: none"> • Issue statement • Tasks to accomplish • Timelines • Deliverables | Specified at Call Order level | Specified at Call Order level |

| | | | | |
|---|----------|-------------------------------------|---|--|
| | | (output) | | |
| 5 | 5.3.1 b. | Status Report on contract execution | Weekly within three (3) business days of the following week | COR, Contracting Officer, FEMA Project Manager and COR |

Part 11
Performance Requirements Summary

11.0 PERFORMANCE REQUIREMENTS SUMMARY (PRS).

The PRS establishes key elements of Contractor performance that represent “mission essential” service requirements, which are identified in the table below in the “Service Output” column. The “Performance Objective” column represents the standard against which Contractor performance will be measured in relation to accomplishment of the corresponding service output. The performance objective or “standard” describes the minimum acceptable level of service by the Contractor for satisfactory performance. The “Acceptable Quality Level (AQL)” column displays the maximum allowable deviation from the performance objective, which, if exceeded, evokes the negative incentive specified in the table below.

| Service Output | Performance Objective | Acceptable Quality Level (AQL) | Method of Inspection | Positive Incentive | Negative incentive | |
|--|--|--|---------------------------|---|---|--|
| | | | | | | |
| 1. Corrective Action Plans and Verification & Validation (V&V) (PWS 5.2) | Contractor shall provide support in the development of CAP/MAPs/MAPs to accurately identify any significant deficiencies or material weaknesses identified during the external audit and internal control assessments and V&V testing. | DHS deadlines are met on time and not any later than two business days after due date. In addition, progress submissions will have no more than 2 major revisions (major meaning no more than 3 corrections) | Direct Observation | Positive Past Performance Review in CPARS | Negative Past Performance Review in CPARS | |
| | | | Progress Reports/Meetings | Exercise of Option Year | Not Exercising an Option Year | |

| | | | | | | |
|-----------------------------------|--|--|---------------------------|---|---|--|
| | | | Quality control Reviews | | Termination of contract | |
| 6. Technical Assistance (PWS 5.3) | Contractor shall provide assessment expertise, programmatic knowledge, and technical CAP/MAP abilities to accurately respond to any ad-hoc analysis and program support request involving IT or Non-IT internal controls in accordance with the PWS. | DHS deadlines are met on time and not any later than two business days after due date. In addition, progress submissions will have no more than 2 major revisions (major meaning no more than 3 corrections) | Direct Observation | Positive Past Performance Review in CPARS | Negative Past Performance Review in CPARS | |
| | | | Progress Reports/Meetings | Exercise of Option Year | Not Exercising an Option Year | |
| | | | Quality control Reviews | | | |
| | | | | | Termination of contract | |

D - Packaging and Marking

SECTION D: Packaging and Marking

If required for the delivery of items, and unless otherwise specified by Government representative, data items shall be preserved, packaged, packed and marked only to the extent necessary to assure carrier acceptance and safe delivery to destination at the lowest rates in compliance with the requirements of the carrier rules and regulations applicable to the mode of transportation.

E - Inspection and Acceptance

SECTION E: Inspection and Acceptance

E.1 INSPECTION AND ACCEPTANCE

The inspection and acceptance of work performed shall be at the site where work is performed. The Government shall have the right to inspect the contractor's performance under this Call Order in accordance with the Inspection and Acceptance clauses. The contracting officer (CO) may conduct such inspection and surveillance of the contractor's performance under the Call Order as determined appropriate and necessary. The CO shall exercise those responsibilities through his staff and in connection with an Inspector General (IG) and any related agencies necessary to ensure that the standards set forth herein are met. The standards set forth in this Call Order shall be the criteria by which the contractor's performance shall be inspected. These standards may either be in full text or incorporated by reference (regulations, etc.). Government inspection personnel may monitor the contractor's performance by physical inspection, review of reports and documentation as well as validated customer complaints. Corrective action for deficiencies shall be at the government's discretion. Government waiver of a deficiency in one call order does not constitute waiver of the requirement for future call orders.

E.2 APPOINTMENT OF CONTRACTING OFFICER'S REPRESENTATIVE (COR) AND/OR ASSISTANT CONTRACTING OFFICER'S REPRESENTATIVE (ACOR)

The CO shall designate individual(s) to act as the COR and/or ACOR under any resultant task order. Letter from the CO shall designate such representative with an information copy to the contractor. The COR shall represent the CO in the "TECHNICAL PHASES" of the work, BUT SHALL NOT BE AUTHORIZED to change any of the terms and conditions of the contract. The COR/ACOR shall be in a liaison capacity to coordinate activities between the contractor and the Government as required in the performance of work under this task order.

E.3 INSPECTION METHODOLOGY

The contractor's inspection methodology shall contain measures for prompt detection of any condition that fails to conform to the BPA / BPA Call requirements. Corrective action procedure shall include, at a minimum, action to correct the deficiency and necessary measures to prevent recurrence of such deficiencies.

INSPECTION AND ACCEPTANCE TERMS

Supplies/Services will be inspected/accepted at:

| CLIN | INSPECTION AT | INSPECTION BY | ACCEPT AT | ACCEPT BY |
|------|---------------|---------------|-------------|------------|
| 0001 | Destination | Government | Destination | Government |
| 0002 | Destination | Government | Destination | Government |

F - Deliveries or Performance

SECTION F: Deliveries or Performance

PERFORMANCE

F.1 PERIOD OF PERFORMANCE

The ordering period of Blanket Purchase Agreement (BPA) is for five (5) years unless the BPA is terminated. The BPA may be terminated for convenience or cause.

F.2 PLACE OF PERFORMANCE

Services may be required at any locations within the United States and its territories. The place(s) of performance are designated in the PWS of this call order.

DELIVERY INFORMATION

| CLIN | DELIVERY DATE | QUANTITY | SHIP TO ADDRESS |
|------|-----------------------------------|----------|---|
| 0001 | POP 16-JUN-2023 TO 15-JUN-2028 | N/A | HQ, FEMA FERGUSON, CHERYL 500 C STREET SW WASHINGTON, DC 20472 PHONE NUMBER FOB: Destination |
| 0002 | POP 16-JUN-2023 TO 15-JUN-2028 | N/A | (SAME AS PREVIOUS LOCATION) FOB: Destination |

G - Contract Administration Data

SECTION G: Contract Administration Data

INVOICE INSTRUCTIONS

The contractor shall submit an invoice(s) upon delivery and acceptance of all supplies or services as specified in the Price/Cost Schedule. Invoices shall include the contract and/or order number. In addition, any packaging with commodities shall also include the contract and/or purchase order number.

Contractors shall submit vouchers electronically in pdf format to the FEMA Finance Center at FEMA-Finance-Vendor-Payments@fema.dhs.gov.

AND

Contractors shall also submit an electronic pdf copy to FEMA COR or program person if a COR is not designated at their email address.

The submission of vouchers electronically will reduce correspondence and other causes for delay to a minimum and will facilitate prompt payment to the Contractor. Paper vouchers mailed to the finance center will not be processed for payment. If the Contractor is unable to submit a payment request in electronic form, the contractor shall submit the payment request using a method mutually agreed to by the Contractor, the Contracting Officer, and the payment office.

Invoices shall be submitted as follows: Contractors shall use Standard Form (SF) 1034 (Public Voucher for Purchases and Services Other Than Personal) and SF 1035 (Continuation Sheet) when requesting payment for supplies or services rendered. Both forms are located at <http://www.gsa.gov/portal/forms/type/SF>. Suitable self-designed forms (contractor invoice forms) may be submitted instead of the SF 1035 as long as they contain the information required.

The voucher must provide a description of the supplies or services, by line item (if applicable), quantity, unit price, and total amount. The item description, unit of measure, and unit price must match those specified in the contract. Invoices that do not match the line item pricing in the contract will be considered improper and will be returned to the Contractor. The Contractor shall not be paid more frequently than on a monthly basis.

SF 1034 and 1035 instructions:

SF 1034 – Public Voucher for Purchases and Services Other than Personal

The information which a contractor is required to submit in its Standard Form 1034 is set forth as follows:

- (1) U.S. Department, Bureau, or establishment and location insert the names and address of the servicing finance office unless the contract specifically provides otherwise.
- (2) Date Voucher Prepared - insert date on which the public voucher is prepared and submitted.
- (3) Contract/Delivery Order Number and Date - insert the number and date of the contract and delivery order, if applicable, under which reimbursement is claimed.
- (4) Requisition Number and Date - leave blank.
- (5) Voucher Number - insert the appropriate serial number of the voucher. A separate series of consecutive numbers, beginning with Number 1, shall be used by the contractor for each new contract. When an original voucher was submitted, but not paid in full because of suspended costs, resubmission vouchers should be submitted in a separate invoice showing the original voucher number and designated with the letter "R" as the last character of the number. If there is more than one resubmission, use the appropriate suffix (R2, R3, etc.)
- (6) Schedule Number; Paid By; Date Invoice Received - leave blank.

- (7) Discount Terms - enter terms of discount, if applicable.
- (8) Payee's Account Number - this space may be used by the contractor to record the account or job number(s) assigned to the contract or may be left blank.
- (9) Payee's Name and Address - show the name of the contractor exactly as it appears in the contract and its correct address, except when an assignment has been made by the contractor, or the right to receive payment has been restricted, as in the case of an advance account. When the right to receive payment is restricted, the type of information to be shown in this space shall be furnished by the Contracting Officer.
- (10) Shipped From; To; Weight Government B/L Number - insert for supply contracts.
- (11) Date of Delivery or Service - show the month, day and year, beginning and ending dates of supplies or services delivered.
- (12) Articles and Services - insert the following: "For detail, see Standard Form 1035" OR "For detail, see contractor invoice form".
- (13) Type the following certification, signed by an authorized official, on the face of the Standard Form 1034.

"I certify that all payments requested are for appropriate purposes and in accordance with the agreements set forth in the contract."

(Name of Official) (Title)

- (14) Amount - insert the amount claimed for the period indicated in (11) above. This amount should be transferred from the total per the SF 1035 Continuation Sheet or contractor invoice form.

SF 1035 – Continuation Sheet

The SF 1035 will be used to identify the specific item description, quantities, unit of measure, and prices for each category of deliverable item or service. Suitable self-designed forms (contractor invoice form) may be submitted instead of the SF 1035 as long as they contain the information required.

The information which a contractor is required to submit in its Standard Form 1035 is set forth as follows:

U.S. Department, Bureau, or Establishment - insert the name and address of the servicing finance office.

Voucher Number - insert the voucher number as shown on the Standard Form 1034.

Schedule Number - leave blank.

Sheet Number - insert the sheet number if more than one sheet is used in numerical sequence. Use as many sheets as necessary to show the information required.

Number and Date of Order - insert payee's name and address as in the Standard Form 1034.

Articles or Services - insert the contract number as in the Standard Form 1034, and description.

Quantity; Unit Price – insert for supply contracts.

Amount - insert the total quantities contract value, and amount and type of fee payable (as applicable).

A summary of claimed current and cumulative goods and services delivered and accepted to date. -

Invoices shall include an itemization of all goods and services delivered and accepted for the period by item and by CLIN. Each invoice shall include sufficient detail to identify goods and services as compared

ELECTRONIC FUNDS TRANSFER (EFT) INFORMATION

1. To receive payment, the contractor shall submit their EFT information to the Government. EFT information may be submitted by EFT form, through System for Award Management (SAM), or on invoice. Failure to provide the EFT information or failure to notify the Government of changes to this EFT information may result in delays in payments and/or rejection of the invoice in accordance with the Prompt Payment clause of this contract. EFT forms may be submitted directly to the FEMA Finance Center at FEMA-Finance-RecordsMaintenance@fema.dhs.gov, or to the Contracting Office.
2. If submitting EFT information on invoice/voucher, the following EFT information should be submitted:

(a) Routing Transit Number (RTN) – The contractor shall provide the current 9-digit RTN of the payee's bank

(b) Payee's account number

(c) Contractor's Tax Identification Number (TIN)

(The EFT information submitted must be that of the contractor unless there is an official Assignment of Claims on file with the payment office.)

If at any time during the term of this contract, the contractor changes any EFT information, (i.e. financial agent, RTN, account number, etc.) the new EFT information must replace the old EFT information on subsequent invoices submitted under this contract, through SAM, or by submission of a new EFT form.

H - Special Contract Requirements

Section H:

508 INFORMATION TECHNOLOGY CLAUSE

<https://www.dhs.gov/compliance-test-processes>

DHS 508 Tool: <https://www.dhs.gov/xlibrary/oast/DART/>

Note: The 508 IT clause is generated from the DHS 508 Tool on an ad hoc basis.
The 508 IT clause generated from the DHS 508 Tool is inserted into the PWS or SOO or SOW.

Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance

criteria.

36 CFR 1194.23 Telecommunications Products applies to all telecommunications products including end-user interfaces such as telephones and non-end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

Enterprise Architecture (EA) Compliance Language

This is a list of EA Architecture Compliance language agreed upon between Components and HQ DHS to be used in preparing SOW, PWS & SOO for IT acquisitions & services. The following Components (CBP,

TSA & USCG) have their own customized version listed below that must be used. All other Components must use the DHS Enterprise Architecture Compliance language that follows:

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Standard Security Language

1. Background Investigations

All contractor personnel who require access to DHS or FEMA information systems, routine access to DHS or FEMA facilities, or access to sensitive information, including but not limited to Personally Identifiable Information (PII), shall be subject to a full background investigation commensurate with the level of the risk associated with the job function or work being performed. FEMA's Personnel Security Division (PSD) will determine the risk designation for each contractor position by comparing the functions and duties of the position against those of a same or similar federal position, applying the same standard for evaluating the associated potential for impact on the integrity and efficiency of federal service.

a. Low Risk without Information System Access

Contractor personnel occupying positions or performing functions with a Low Risk designation and who do not require access to DHS or FEMA information systems shall undergo a National Agency Check with Inquiries (NACI) Tier 1 and a credit check and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

b. Low Risk with Information System Access

Contractor personnel occupying positions or performing functions with a Low Risk designation and who require access to DHS or FEMA information systems shall undergo a Tier 2 Suitability Background Investigation (T2S) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

c. Moderate Risk

Contractor personnel occupying positions or performing functions with a Moderate Risk designation shall undergo a Tier 2 Suitability Background Investigation (T2S) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

d. High Risk

Contractor personnel occupying positions or performing functions with a High Risk designation shall undergo a Tier 4 Background Investigation (BI) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

2. Background Investigation Process

Contractors performing on this contract must be United States Citizens. Contractor applicants must also be eighteen (18) years of age or older to allow for the conduct of certain security related queries.

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 121-3-1-6, "Contractor Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 121-3-1-6 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

Contractor personnel who already have a favorably adjudicated background investigation may be eligible to perform work under this contract without further processing by FEMA PSD if:

- § the investigation was completed within the last five years;
- § it meets or exceeds the minimum requirement for the position they will occupy or functions they will perform on this contract;
- § the contractor personnel have not had a break in employment since the prior favorable adjudication; and,
- § FEMA PSD has verified the investigation and confirmed that no new derogatory information has been disclosed which may require a reinvestigation.

FEMA PSD will notify the COR of the names of the contractor personnel eligible to work based on prior, favorable adjudication. The COR will, in turn, notify the Contractor of the names of the favorably adjudicated contractor personnel, at which time the favorably adjudicated contractor personnel will be eligible to begin work under this contract.

For those contractor personnel who do not have an acceptable, prior, favorable adjudication or who otherwise require reinvestigation, FEMA PSD will issue an electronic notification via email to the contractor personnel that contains the following documents, which are incorporated into this contract by reference, along with a link to the Office of Personnel Management's (OPM) Electronic Questionnaires for Investigation Processing (e-QIP) system and instructions for submitting the necessary information:

- § Standard Form 85P, "Questionnaire for Public Trust Positions"
- § Optional Form 306, "Declaration for Federal Employment"
- § SF 87, "Fingerprint Card" (2 copies)
- § DHS Form 11000-6, "Non-Disclosure Agreement"
- § DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Applicants born outside the United States will be required to provide proof of citizenship in the form of a Certificate of Naturalization (Form N550 or N570), an unexpired U.S. Passport, or State Department issued Consular Report of Birth Abroad (CRBA) (FS-240).

FEMA PSD will only accept complete packages consisting of all of the above documents and Standard Form 85P, which must be completed electronically through the OPM's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background

information.

Residency requirements apply to the background investigation process. Persons subject to investigation and final adjudication for fitness or suitability must have lived within the United States for no less than 3 of the last 5 years as defined in the DHS Instruction 121-01-007-01, The Department of Homeland Security, Personnel Security, Suitability and Fitness Program (June 14, 2016). DHS has determined this to be the amount of time required to be the sufficient minimum investigative period for the purpose of performing a suitability or fitness adjudication. Both OPM and OMB require a final adjudicative decision to support the issuance of the HSPD-12 compliant PIV Card that contractors are issued by FEMA Physical Security.

Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contractor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in an unfavorable determination FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

3. Continued Eligibility and Reinvestigation

Eligibility determinations based on a T1, T2S, or T4 (or the equivalent OPM investigation) are valid for five years from the date that the investigation was completed and closed. Contractor personnel required to undergo a background investigation to perform work under this contract shall be ineligible to perform work under this contract upon the expiration of the background investigation unless and until the contractor personnel have undergone a reinvestigation and FEMA's Personnel Security Division has renewed their eligibility to perform work under this contract.

4. Exclusion by Contracting Officer

The Contracting Officer, independent of FEMA's Personnel Security Division, may direct the Contractor be excluded from working on this contract. Any contractor found or deemed to be unfit or whose continued employment on the contract is deemed contrary to the public interest or inconsistent with the best interest of the agency may be removed.

5. Facility Access

The Contractor shall comply with FEMA Directive 121-1 "FEMA Personal Identity Verification Guidance," FEMA Directive 121-3 "Facility Access," and FEMA Manual 121-3-1 "FEMA Credentialing Access Manual," to arrange for contractor personnel's access to FEMA facilities, which includes, but is not limited to, arrangements to obtain any necessary identity badges for contractor personnel.

Contractor personnel working within any FEMA facility who do not require access to DHS or FEMA IT systems and do not qualify for a PIV Card may be issued a Facility Access Card (FAC). FACs cannot exceed 180 days; all contractors requiring access greater than 180 days will need to qualify for and receive

a PIV card before being allowed facility access beyond 180 days.

Contractor personnel shall not receive a FAC until they have submitted a SF 87, "Fingerprint Card," and an OF306, "Declaration for Federal Employment," and receive approval from FEMA PSD. Contractor personnel using a FAC for access to FEMA facilities must be escorted in Critical Infrastructure areas (i.e., server rooms, weapons rooms, mechanical rooms, etc.) at all times.

FEMA may deny facility access to any contractor personnel whom FEMA's Office of the Chief Security Officer (OCSO) has determined to be a potential security threat.

6. Separation From Contract

The Contractor shall notify the FEMA COR of all terminations/resignations within five calendar days of occurrence. The Contractor must account for all forms of Government-provided identification issued to contractor employees under a contract (i.e., the PIV cards or other similar badges) and must return such identification to FEMA as soon as any of the following occurs:

- § When no longer needed for contract performance.
- § Upon completion of a contractor employee's employment.
- § Upon contract completion or termination.

If an identification card or building pass is not available to be returned, the Contractor shall submit a report to the FEMA COR, referencing the pass or card number, name of the individual to whom it was issued, and the last known location and disposition of the pass or card.

The Contractor or contractor personnel's failure to return all DHS- or FEMA-issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS or FEMA may subject the contractor personnel and the Contractor to civil and criminal liability.

7. Standard Operations Security Program (OPSEC) Training Language

Contractors and Subcontractors who are working on this contract shall receive the OPSEC Awareness Brief. Access to the briefing can be obtained at <http://cdsetrain.dtic.mil/opsec>. Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

8. OCSO Required Language for Contracts Including "For Official Use Only" (FOUO) Information

In accordance with DHS Management Directive 11042.1 contractors, consultants and others to whom access is granted will abide by 11042.1; DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities. The contractor will:

- 1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.**
- 2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.**
- 3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.**
4. Contractors and Consultants shall:
 1. Execute a DHS Form 11000-6, Sensitive but Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be

granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

9. Unauthorized Disclosure of Classified or Unclassified Information

All contractors and subcontractors are required to train on Unauthorized Disclosure of Classified or Unclassified Information to perform duties established by the Government during the performance period of and execution of this contract. Access to the training can be obtained at: <https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm>. Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

10. Government-Furnished Equipment and Information

Privacy Considerations

To accomplish the tasks outlined in this contract, the contractors will have access to PII of first name, last name, email addresses, and work phone numbers of FEMA employees via Global Address List (GAL) by way of FEMA laptops use. The information sharing is authorized by Routine Use F of [DHS/ALL-014 Department of Homeland Security Personnel Contact Information](#)" March 16, 2018 83 FR 11780. The information sharing is also covered by the following Privacy Impact Assessments: DHS/ALL/PIA-015 Web Portal, DHS/ALL/PIA-059 Employee Collaboration Tool.

The contractor will limit access to the PII provided by FEMA under this contract only to the contractor's authorized personnel who need to know the information to accomplish the tasks outlined in this contract.

The contractor shall ensure no computer matching, as that term is defined in 5 U.S.C. § 552a(o), will occur for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs.

If at any time during the term of this contract any part of FEMA PII, in any form, that the contractor obtains from FEMA ceases to be required by the contractor for the performance of the contract, or upon termination of the contract, whichever occurs first, the contractor shall, within fourteen (14) days thereafter, promptly notify FEMA and securely return PII to FEMA, or, at FEMA's written request destroy, un-install and/or remove all copies of such PII in the contractor's possession or control, and certify in writing to FEMA that such tasks have been completed."

11. Safeguarding of Sensitive Information

a. Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

b. Definitions. As used in this clause—

"Personally identifiable information" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of personally identifiable information is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become

personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

1. Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
2. Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
3. Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
4. Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

1. ***Truncated SSN (such as last 4 digits)***
2. ***Date of birth (month, day, and year)***
3. ***Citizenship or immigration status***
4. ***Ethnic or religious affiliation***
5. ***Sexual orientation***

6. ***Criminal History***
7. ***Medical Information***
8. ***System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)***

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

c. Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at [www...](http://www.dhs.gov), or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

d. Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

1. Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

2. The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

3. All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Sensitive but Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

4. The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

e. Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component Chief Information Officer (CIO), or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified, the ATO is valid for three (3) years. The Contractor shall adhere to current FedRAMP and/or Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

1. Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 9.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.0, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

i. Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Security Requirements Traceability Matrix and Government security documentation templates, as adapted for Contractor IT systems. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

ii. Independent Assessment. Contractors 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 SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance. The government shall perform all required independent verification and validation (IV&V) activities for systems on premise or cloud hosted for all security reauthorization or security assessments for major system modifications.

iii. Support the completion of the Privacy Threshold Analysis (PTA) when completion of a PTA is required in the solicitation. As part of the SA process, the Contractor may be required to support the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

f. Renewal of ATO. Unless otherwise directed by the Contracting Officer, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA

documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

g. Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

h. Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

i. Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal Information Security Management Act (FISMA) reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy FISMA reporting requirements for Contractor systems.

j. Sensitive Information Incident Reporting Requirements.

1. All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

2. If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- i. Data Universal Numbering System (DUNS).
- ii. Contract numbers affected unless all contracts by the company are affected.
- iii. Facility CAGE code if the location of the event is different than the prime contractor location.
- iv. Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email).
- v. Contracting Officer POC (address, telephone, email).
- vi. Contract clearance level.
- vii. Name of subcontractor and CAGE code if this was an incident on a subcontractor network.
- viii. Government programs, platforms or systems involved.
- ix. Location(s) of incident.
- x. Date and time the incident was discovered.
- xi. Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level.
- xii. Description of the Government PII and/or SPII contained within the system.
- xiii. Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system.
- xiv. Any additional information relevant to the incident.

k. Sensitive Information Incident Response Requirements.

1. All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

2. The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

3. Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- i. Inspections,
- ii. Investigations,
- iii. Forensic reviews, and
- iv. Data analyses and processing.

4. The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

l. Additional PII and/or SPII Notification Requirements.

2. The Contractor shall have in place procedures and the CAP/MA Pability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and

subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

l. Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

1. A brief description of the incident.
2. A description of the types of PII and SPII involved.
3. A statement as to whether the PII or SPII was encrypted or protected by other means.
4. Steps individuals may take to protect themselves.
5. What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
6. Information identifying who individuals may contact for additional information.

m. Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

1. Provide notification to affected individuals as described above; and/or

2. Provide credit monitoring services to individuals whose data resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

1. Triple credit bureau monitoring.
2. Daily customer service.
3. Alerts provided to the individual for changes and fraud; and
4. Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

3. Establish a dedicated call center. Call center services shall include:

- i. A dedicated telephone number to contact customer service within a fixed period.
- ii. Information necessary for registrants/enrollees to access credit reports and credit scores.
- iii. Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics.
- iv. Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate.
- v. Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- vi. Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(n) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

12. Information Technology Security and Privacy Training (Mar 2015)

a. Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

b. Security Training Requirements.

1. All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

2. The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources CAP/MAPable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

c. Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

“The contractor will limit access to the PII provided by FEMA under this contract only to the contractor’s authorized personnel who need to know the information to accomplish the tasks outlined in this contract.

The contractor shall ensure no computer matching, as that term is defined in 5 U.S.C. § 552a(o), will occur for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs.

If at any time during the term of this contract any part of FEMA PII, in any form, that the contractor obtains from FEMA ceases to be required by the contractor for the performance of the contract, or upon termination of the contract, whichever occurs first, the contractor shall, within fourteen (14) days thereafter, promptly notify FEMA and securely return PII to FEMA, or, at FEMA's written request destroy, un-install and/or remove all copies of such PII in the contractor's possession or control, and certify in writing to FEMA that such tasks have been completed."

13. Records Management Obligations

A. Applicability

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

B. Definitions

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

The term Federal record:

1. includes FEMA records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their FEMA contract.
4. may include deliverables and documentation associated with deliverables.

C. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.
3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. FEMA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of FEMA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to FEMA. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the PWS. The Contractor shall ensure that the appropriate personnel, administrative, technical, and

physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the PWS. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and FEMA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with FEMA policy.

8. The Contractor shall not create or maintain any records containing any non-public FEMA information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. The FEMA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which FEMA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

14. Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at <https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

2. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at <https://www.dhs.gov/508-testing>.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

a. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018.

Instructions to Offerors

For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

- a. Accessibility test results based on the required test methods.
- b. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- c. Documentation of core functions that cannot be accessed by persons with disabilities.
- d. Documentation on how to configure and install the ICT Item to support accessibility.
- e. Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
- f. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

15. Government Responsibilities

The Government shall provide a government owned computer to help facilitate access to government email, documents, and standard operating procedures in helping him/her to provide services as listed under this PWS.

16. Security

All personnel require access to information up to the sensitive but unclassified, for official use only (FOUO) levels. Contractor must ensure contractor employees receive a favorably adjudicated public trust suitability prior to entry on duty (EOD). All individuals will be U.S. citizens. The contractor shall follow the standards established within DHS and FEMA policy.

Unauthorized Disclosure of Classified or Unclassified Information:

Contractors and Subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training.

Access to the training can be obtained

at: <https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm>

Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

OPSEC Training:

Contractors and Subcontractors who are working on this contract shall receive the OPSEC Awareness Brief.

Access to the briefing can be obtained at <http://cdsetrain.dtic.mil/opsec>

Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30

calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

Insider Threat Training:

Insider Threat training for Contractors can be found at: <http://cdsetrain.dtic.mil/itawareness/index.htm>.

Certificate of training is required for all cleared contractor employees who are working with classified or unclassified information. All certificates must be sent to the assigned FEMA Contracting Officer Representative, before the Contractor or Subcontractor is granted access to classified or unclassified information but no later than 30 calendar days after awarded contract. All cleared contractor personnel are required to recertify Insider Threat training annually thereafter. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

For Official Use Only (FOUO) Information:

In accordance with DHS Management Directive 11042.1 contractors, consultants and others to whom access is granted will abide by 11042.1; DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

The contractor will:

Be aware of and comply with the safeguarding requirements for “For Official Use Only” (FOUO) information as outlined in this directive.

Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.

Be aware that divulging information without proper authority could result in administrative or disciplinary action.

Contractors and Consultants shall execute a DHS Form 11000-6, *Sensitive but Unclassified Information Non Disclosure Agreement* (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon date of the DHS Policy and not applied retroactively.

Foreign Travel and Government-Issued Equipment

Per DHS and FEMA IT policy, FEMA employees and contractors are not authorized to take government-issued equipment, including cell phones, computers, or tablets such as iPads, outside of the United States regardless of the reason for travel. If government-issued equipment is required for official foreign travel, FEMA government employees may request a temporary loaner device through the [Mobility Service Center](#). Office of the Chief Information Officer, Service Center for the duration of their trip. FEMA contractors must contact their contracting officer’s representative (COR) for further guidance.

If your device is detected as operating outside of the United States and its territories it will be disabled, and your information will be forwarded to the Office of Professional Responsibility for review.

Background Investigations

All contractor personnel who require access to DHS or FEMA information systems, routine access to DHS or FEMA facilities, or access to sensitive information, including but not limited to Personally Identifiable Information (PII), shall be subject to a full background investigation commensurate with the level of the risk associated with the job function or work being performed. FEMA’s Personnel Security Division (PSD) will determine the risk designation for each contractor position by comparing the functions and

duties of the position against those of a same or similar federal position, applying the same standard for evaluating the associated potential for impact on the integrity and efficiency of federal service.

Low Risk without Information System Access

Contractor personnel occupying positions or performing functions with a Low-Risk designation and who do not require access to DHS or FEMA information systems may undergo a Tier 1 investigation with a credit check and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract. (also reference Facility Access).

Low Risk with Information System Access

Contractor personnel occupying positions or performing functions with a Low-Risk designation and who require access to DHS or FEMA information systems shall undergo a Tier 2 Suitability Background Investigation (T2) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

Moderate Risk

Contractor personnel occupying positions or performing functions with a Moderate Risk designation shall undergo a Tier 2 Suitability Background Investigation (T2) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

High Risk

Contractor personnel occupying positions or performing functions with a High-Risk designation shall undergo a Tier 4 Suitability Background Investigation (T4) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

Background Investigation Process

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 121-3-1-6,

"Contract Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 121-3-1-6 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

Contractor personnel who already have a favorably adjudicated background investigation, may be eligible to perform work under this contract without further processing by FEMA PSD if:
the investigation was completed within the last five years,
it meets or exceeds the minimum requirement for the position they will occupy or functions they will perform on this contract,
the contractor personnel have not had a break in employment since the prior favorable adjudication, and,

FEMA PSD has verified the investigation and confirmed that no new derogatory information has been disclosed which may require a reinvestigation.

FEMA PSD will notify the COR of the names of the contractor personnel eligible to work based on prior, favorable adjudication. The COR will, in turn, notify the Contractor of the names of the favorably adjudicated contractor personnel, at which time the favorably adjudicated contractor personnel will be eligible to begin work under this contract.

For those contractor personnel who do not have an acceptable, prior, favorable adjudication or who

otherwise require reinvestigation, FEMA PSD will issue an electronic notification via email directly to the contractor applicant/personnel that contains the following documents, which are incorporated into this contract by reference, along with a link to the Office of Personnel Management's (OPM) Electronic Questionnaires for Investigation Processing (e-QIP) system and instructions for submitting the necessary information:

Standard Form 85P, "Questionnaire for Public Trust Positions"

Optional Form 306, "Declaration for Federal Employment"

SF 87, "Fingerprint Card" (2 copies)

DHS Form 11000-6, "Non-Disclosure Agreement"

DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the Office of Personnel Management's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.

Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contractor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in an unfavorable determination

FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

Continued Eligibility and Reinvestigation

Eligibility determinations based on a Low Risk T1, Moderate Risk T2S or High Risk T4 are valid for five years from the date that the investigation was completed and closed. Contractor personnel required to undergo a background investigation to perform work under this contract shall be ineligible to perform work under this contract upon the expiration the background investigation unless and until the contractor personnel have undergone a reinvestigation and FEMA's Personnel Security Division has renewed their eligibility to perform work under this contract.

Exclusion by Contracting Officer

The Contracting Officer, independent of FEMA's Personnel Security Division, may direct the Contractor

be excluded from working on this contract. Any contractor found or deemed to be unfit or whose continued employment on the contract is deemed contrary to the public interest or inconsistent with the best interest of the agency may be removed

I - Contract Clauses

52.202-1 Definitions. (JUN 2020)

52.203-3 Gratuities. (APR 1984)

52.203-5 Covenant Against Contingent Fees. (MAY 2014)

52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights. (JUN 2020)

52.204-4 Printed or Copied Double-Sided on Postconsumer Fiber Content Paper. (MAY 2011)

52.204-9 Personal Identity Verification of Contractor Personnel. (JAN 2011)

52.204-13 System for Award Management Maintenance. (OCT 2018)

52.204-18 Commercial and Government Entity Code Maintenance. (AUG 2020)

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities. (NOV 2021)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (NOV 2021)

52.209-10 Prohibition on Contracting With Inverted Domestic Corporations. (NOV 2015)

52.212-4 Contract Terms and Conditions - Commercial Products and Commercial Services. (DEC 2022)

52.224-1 Privacy Act Notification. (APR 1984)

52.224-2 Privacy Act. (APR 1984)

52.225-13 Restrictions on Certain Foreign Purchases. (FEB 2021)

52.227-14 Rights in Data-General. (MAY 2014)

52.228-4 Workers' Compensation and War-Hazard Insurance Overseas. (APR 1984)

52.229-1 State and Local Taxes. (APR 1984)

52.232-1 Payments. (APR 1984)

52.232-39 Unenforceability of Unauthorized Obligations. (JUN 2013)

52.233-1 Disputes. (MAY 2014)

52.233-3 Protest After Award. (AUG 1996)

52.233-4 Applicable Law for Breach of Contract Claim. (OCT 2004)

52.237-3 Continuity of Services. (JAN 1991)

52.242-13 Bankruptcy. (JUL 1995)

52.244-6 Subcontracts for Commercial Products and Commercial Services. (DEC 2022)

52.245-1 Government Property. (SEP 2021)

52.245-9 Use and Charges. (APR 2012)

52.251-1 Government Supply Sources. (APR 2012)

52.204-2 Security Requirements. (MAR 2021)

(a) This clause applies to the extent that this contract involves access to information classified *Confidential*, *Secret*, or *Top Secret*.

(b) The Contractor shall comply with (1) the Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (32 CFR part 117), and (2) any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of clause)

52.204-21 Basic Safeguarding of Covered Contractor Information Systems. (NOV 2021)

(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 products or commercial services, 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.

(End of clause)

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders - Commercial Products and Commercial Services. (DEC 2022)

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

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

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (NOV 2021) (Section 1634 of Pub. L. 115-91).

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

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(5) 52.233-3, 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 and 108-78 (19 U.S.C. 3805 note)).

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

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

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

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

[X] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 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).

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

[X] (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (NOV 2021) (31 U.S.C. 6101 note).

☒ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018) (41 U.S.C. 2313).

☐ (10) (Reserved)

☐ (11) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (OCT 2022) (15 U.S.C. 657a).

☐ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2022) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

☐ (13) (Reserved)

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

☐ (ii) Alternate I (MAR 2020) of 52.219-6.

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

☐ (ii) Alternate I (MAR 2020) of 52.219-7.

☐ (16) 52.219-8, Utilization of Small Business Concerns (OCT 2022) (15 U.S.C. 637(d)(2) and (3)).

☐ (17)(i) 52.219-9, Small Business Subcontracting Plan (OCT 2022) (15 U.S.C. 637(d)(4)).

☐ (ii) Alternate I (NOV 2016) of 52.219-9.

☐ (iii) Alternate II (NOV 2016) of 52.219-9.

☐ (iv) Alternate III (JUN 2020) of 52.219-9.

☐ (v) Alternate IV (SEP 2021) of 52.219-9.

☐ (18)(i) 52.219-13, Notice of Set-Aside of Orders (MAR 2020) (15 U.S.C. 644(r)).

☐ (ii) Alternate I (MAR 2020) of 52.219-13.

☐ (19) 52.219-14, Limitations on Subcontracting (OCT 2022) (15 U.S.C. 657s).

☐ (20) 52.219-16, Liquidated Damages-Subcontracting Plan (SEP 2021) (15 U.S.C. 637(d)(4)(F)(i)).

☐ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (OCT 2022) (15 U.S.C. 657f).

☐ (22)(i) 52.219-28, Post-Award Small Business Program Rerepresentation (OCT 2022) (15 U.S.C. 632(a)(2)).

☐ (ii) Alternate I (MAR 2020) of 52.219-28.

☐ (23) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (OCT 2022) (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 (OCT 2022) (15 U.S.C. 637(m)).

[] (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (MAR 2020) (15 U.S.C. 644(r)).

[] (26) 52.219-33, Nonmanufacturer Rule (SEP 2021) (15 U.S.C. 657s).

[X] (27) 52.222-3, Convict Labor (JUN 2003) (E.O. 11755).

[X] (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (DEC 2022) (E.O. 13126).

[X] (29) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

[X] (30)(i) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

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

[X] (31)(i) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

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

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

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

[X] (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 (NOV 2021) (22 U.S.C. chapter 78 and E.O. 13627).

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

[] (36) 52.222-54, Employment Eligibility Verification (MAY 2022). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR 22.1803.)

[] (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 Televisions (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).

[] (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. 13693).

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

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

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

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

[] (49)(i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (DEC 2022) (19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, 19 U.S.C. chapter 29 (sections 4501-4732), Public Law 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

[] (ii) Alternate I [Reserved]

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

[] (iv) Alternate III (JAN 2021) of 52.225-3.

[] (v) Alternate IV (OCT 2022) of 52.225-3.

[] (50) 52.225-5, Trade Agreements (DEC 2022) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

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

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

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

☐ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007) (42 U.S.C. 5150).

☐ (55) 52.229-12, Tax on Certain Foreign Procurements (FEB 2021).

☐ (56) 52.232-29, Terms for Financing of Purchases of Commercial Products and Commercial Services (NOV 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

☐ (57) 52.232-30, Installment Payments for Commercial Products and Commercial Services (NOV 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

☒ (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).

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

☐ (62) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(13)).

☐ (63)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (NOV 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631).

☐ (ii) Alternate I (APR 2003) of 52.247-64.

☐ (iii) Alternate II (NOV 2021) of 52.247-64.

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

☒ (1) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67).

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

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

☒ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

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

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

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

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

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

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

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

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

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

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

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

(ii) 52.203-19, 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 (NOV 2021) (Section 1634 of Pub. L. 115-91).

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

(v) 52.219-8, Utilization of Small Business Concerns (OCT 2022) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting

opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

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

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

(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 (MAY 2022) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022).

(xviii) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2022) (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. Subtitle A, Part V, Subpart G 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 (NOV 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

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

(End of clause)

52.217-8 Option To Extend Services. (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days prior to the period of performance ending.

(End of clause)

52.217-9 Option To Extend the Term of the Contract. (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days prior to the period of performance ending; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of clause)

3052.204-71 Contractor employee access. (SEP 2012)

(a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (DEC 2020)

(a) Definitions. As used in this clause—

“Backhaul” means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

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

“Covered telecommunications equipment or services” means—

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

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications

equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

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

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

“Critical technology” means—

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

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

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

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

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

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

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

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

“Interconnection arrangements” means arrangements governing the physical connection of two or more networks to allow the use of another’s network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

“Reasonable inquiry” means an inquiry designed to uncover any information in the entity’s possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

“Roaming” means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

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

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

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

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

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

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

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

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

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

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

J - List of Documents, Exhibits and Other Attachments

Attachment 1: 1.9.1 OCFO Remediation SCA Wage Determination 2015-4281 (230207-1037)

Attachment 2: 1.14.2 OCFO Remediation Pricing Sheet (230207-1055)

| Attachment Number | Title | Date |
|--------------------------|--------------|-------------|
| | | |

K - Representations, Certifications, and Other Statements of Bidders

52.203-11 Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions. (SEP 2007)

52.204-19 Incorporation by Reference of Representations and Certifications. (DEC 2014)

52.225-25 Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran-Representation and Certifications. (JUN 2020)

52.204-17 Ownership or Control of Offeror. (AUG 2020)

(a) *Definitions.* As used in this provision-

Commercial and Government Entity (CAGE) code means-

- (1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location; or
- (2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

(b) The Offeror represents that it [] has or [] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (c) and if applicable, paragraph (d) of this provision for each participant in the joint venture.

(c) If the Offeror indicates "has" in paragraph (b) of this provision, enter the following information:

Immediate owner CAGE code: []

Immediate owner legal name: [(Do not use a "doing business as" name)]

Is the immediate owner owned or controlled by another entity?: [] Yes or [] No.

(d) If the Offeror indicates "yes" in paragraph (c) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: []

Highest-level owner legal name: [(Do not use a "doing business as" name)]

(End of provision)

52.204-20 Predecessor of Offeror. (AUG 2020)

(a) *Definitions.* As used in this provision-

Commercial and Government Entity (CAGE) code means-

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location; or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

(b) The Offeror represents that it [] is or [] is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(c) If the Offeror has indicated "is" in paragraph (b) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: [(or mark "Unknown")].

Predecessor legal name: [(Do not use a "doing business as" name)].

(End of provision)

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment. (NOV 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its

offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services-Representation, or in paragraph (v)(2)(i) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Products and Commercial Services. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

(a) *Definitions.* As used in this provision-

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to-

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to-

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(d) *Representations.* The Offeror represents that-

(1) It [] will, [] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual

instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that-

It [] does, [] does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.* (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment-

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services-

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment-

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

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services-

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 Covered Telecommunications Equipment or Services-Representation. (OCT 2020)

(a) *Definitions.* As used in this provision, "covered telecommunications equipment or services" and "reasonable inquiry" have the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(c) *Representations.* (1) The Offeror represents that it [] does, [] does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(2) After conducting a reasonable inquiry for purposes of this representation, the offeror represents that it [] does, [] does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services.

(End of provision)

52.209-7 Information Regarding Responsibility Matters. (OCT 2018)

(a) *Definitions.* As used in this provision-

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

Federal contracts and grants with total value greater than \$10,000,000 means-

- (1) The total value of all current, active contracts and grants, including all priced options; and
- (2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [] has [] does not have current active Federal contracts and grants with total value greater than \$10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of \$5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in-

(A) The payment of a monetary fine or penalty of \$5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of \$100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIS as required through maintaining an active registration in the System for Award Management, which can be accessed via <https://www.sam.gov> (see 52.204-7).

(End of provision)

L - Instructions, Conditions, and Notices to Bidders

SECTION L: INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

L.1 The Federal Emergency Management Agency (FEMA) is releasing this Request for Proposal (RFP) in electronic format only. The electronic version of this RFP is the official version for this acquisition. No hard copy of the RFP will be issued. Any amendments to this RFP will be released via the Government's Government Point of Entry (GPE).

L.2 The proposal evaluation and discussion procedures in Federal Acquisition Regulation (FAR) Subpart 15.3 ("Source Selection") applies to the evaluation process of this RFP. The Government will conduct evaluations using a "Best Value" approach. The Government does intend to conduct discussions with offerors in the competitive range. Discussions will be conducted in accordance with FAR 15.306(d).

L.3 COMMUNICATIONS WITH THE GOVERNMENT

L.3.1 Prospective offerors are cautioned against contacting other Government personnel in regard to this solicitation prior to contract award. Prospective offerors are also cautioned to advise potential subcontractors or teaming contractors of this instruction. If such contact occurs and is found to be prejudicial to competing offerors, the offeror (including subcontractors or teaming contractors) making such contact shall be excluded from award consideration.

L.3.2 Point of Contact: The Procuring Contracting Officer (PCO), Shawn Smith, is the point of contact for this acquisition, and can be reached via email at shawn.smith@fema.dhs.gov

L.3.3 Questions: The cutoff date of questions is March 19, 2023 at 11:00 AM ET.

L.3.3.1 Any questions, comments, or requests for clarification(s) regarding this RFP shall be emailed to shawn.smith@fema.dhs.gov and janine.queen@fema.dhs.gov. Any responses to questions will be sent electronically to all offerors via an amendment in betaSAM to this RFP.

L.3.3.2 All questions and requests for clarification(s) shall identify the applicable RFP number in the subject line. In the body of the message references shall identify the RFP section and paragraph number for each question. If attachments are used, they must be in Microsoft Word format (No Charts or Graphs will be accepted).

L.3.4 Discussions: This RFP includes FAR Provision 52.215-1 Alternate I Instructions to Offerors – Competitive Acquisition, which advises the Government intends to conduct discussions with offerors in the Competitive Range, however, the Government reserves the right to award based on initial proposals without holding discussions. Therefore, initial proposals should contain the offeror's best terms from a technical and cost standpoint. Even if the Government does not hold discussions, the Government reserves the right to negotiate with one or more, but not necessarily all offerors, for any reason.

L.4 PROPOSAL PREPARATION COSTS

L.4.1 The Government will not be obligated to pay any costs incurred by an offeror in the preparation and submission of a proposal in response to this RFP. The Contracting Officer (CO) is the only person who can legally bind the Government and obligate the Government for the expenditure of public funds in connection to this procurement.

L.5. PROPOSAL SUBMISSION INSTRUCTIONS

L.5.1 Proposals submitted in response to this RFP shall be formatted as stated below and furnished electronically to shawn.smith@fema.dhs.gov and janine.queen@fema.dhs.gov. Proposals shall only be submitted as described herein.

L.5.2 Proposal Compliance: The Government must have received from the offeror a fully compliant proposal. The proposal is compliant when it conforms to all of the requirements of this RFP which

includes the Performance Work Statement (PWS). The Government may declare an offeror to be unacceptable if it does not meet all such terms and conditions.

L.5.3 Proposal Acceptance: Proposals should have a validity period of no less than 120 days. The offeror shall specify the proposal validity period in the Proposal Summary.

L.5.4 Proposal Retention: In accordance with FAR Subpart 4.8, Government contract files, the Government will retain one copy of all unsuccessful proposals.

L.5.4.1 Late Proposals: Proposals submitted after the exact time and date specified will be considered late and will not be evaluated nor considered for award.

L.5.4.2 Proposals for this RFP are due no later than 11:00 AM, ET on April 8, 2023.

L.6 PROPOSAL PREPARATION INSTRUCTIONS

L.6.1 Proposal Format

L.6.1.1 The acceptable electronic formats for proposals shall be compatible with Microsoft (MS) Office 365, specifically MS Word and MS Excel. All volumes shall be electronic files and not be password protected.

L.6.1.2 Minimum type size shall be 12 point Time New Roman standard font with single spacing (not to exceed 46 lines per page). Typesetting, font compression, or other techniques to reduce character size or spacing are not permitted and are considered a deliberate attempt to circumvent the page limits. Prohibited techniques include setting the paragraph line spacing, a feature of MS Word, "exactly at 12 point." For tables, charts, graphs, and figures, the text shall be no smaller than:

Art: 10 point Times New Roman
Tables: 10 point Times New Roman
Titles: 10 point Times New Roman, bold, initial cap

L.6.1.3 Legible tables, charts, graphs, and figures may be used, wherever practical, to depict organizations, systems, layout, and implementation schedules, etc. These displays shall not exceed 11 by 17 inches in size. Foldout pages may be used only for large tables, charts, graphs, diagrams, and schematics; not for pages of text. Elaborate brochures or documentation, detailed artwork, or other embellishments are unnecessary and are not given extra credit.

L.6.1.4 Files shall be named IAW the file naming conventions shown in Table 2, Proposals File Name Matrix, below. The proposal shall be labeled with the RFP number, as well as the name, address, telephone number, CAGE Code, and UEI Number of the offeror. Pages shall be numbered sequentially by volume.

L.6.1.5 Offerors shall screen all media for computer viruses prior to submission to the Government.

L.6.2 Proposal Content and Organization

L.6.2.1 The offeror shall prepare the proposal set forth in Table L.1, Proposal Organization Table, and Table L.2, Proposal File Name Matrix. The completion and submission to the Government of documents identified in Table 1, Proposal Organization Table, shall constitute an offer and shall indicate the offeror's unconditional consent to the terms and conditions of the RFP.

L.6.2.2 Each volume shall be written or presented on a standalone basis. Information required for proposal evaluation that is not found in its designated volume or presentation will be assumed to have been omitted from the proposal and will not be considered.

L.6.2.3 Pages that exceed the required page limitations set forth in Table L.1, Proposal Organization

Table, will not be evaluated.

L.6.2.4 All electronic files must be submitted using the file names in Table 2, Proposal File Name Matrix, below:

| PROPOSAL ORGANIZATION TABLE | | | |
|-----------------------------|--------------------------------|-------------------|---|
| Vol. No. | Volume Title | No. of Copies | Page Limit |
| 1 | Proposal Summary and Documents | 1 Electronic Copy | None |
| 2 | Technical Proposal | 1 Electronic Copy | 40 Pages Total (exclusive of staffing matrix and resumes) |
| 3 | Past Performance | 1 Electronic Copy | 15 pages |
| 4 | Price Proposal | 1 Electronic Copy | None |

TABLE L.1 PROPOSAL ORGANIZATION TABLE

| PROPOSAL FILE NAME MATRIX | | | |
|---------------------------|-------------------------------|--|--|
| Vol. No. | Volume Name | File Name | Contents |
| 1 | Proposal Summary and Document | (insert Offeror Name) – Proposal Summary.docx | Offeror's Proposal Summary |
| | | (insert Offeror Name) – QCP.docx | Offeror's Quality Control Plan |
| 2 | Technical Proposal | (insert Offeror Name) – PWS Management.docx | Offeror's PWS Management |
| | | (insert Offeror Name) – PWS Staffing Plan.docx | Offeror's PWS Staffing / Surge |
| | | (insert Offeror Name) – Staffing Matrix.xlsx | Offeror's Staffing Matrix Spreadsheet |
| | | (insert Offeror Name) – PWS Live Call Order | Offeror's PWS for Live Call Order |
| 3 | Past Performance | (insert Offeror Name) – References | Offeror's Reference Documents Submitted |
| | | (insert Offeror Name) – CPARS | Offeror's CPARS Documents Submitted |
| | | (insert Offeror Name) – PPQ | Offeror's Past Performance Questionnaire forwarded to Previous Customers |
| 4 | Price Proposal | (insert Offeror Name) – Price Narrative.docx | Offeror's Price Proposal Narrative |

| | | | |
|--|--|------------------------------------|--------------------------------------|
| | | (insert Offeror Name) – Price.xlsx | Offeror's Price Proposal Spreadsheet |
|--|--|------------------------------------|--------------------------------------|

TABLE L.2 PROPOSAL FILE NAME MATRIX

L.6.3 Consistency: Each volume of the offeror's proposal shall be consistent with the other proposal volumes and shall demonstrate the understanding and ability to perform according to the statement of work of the contract. The offeror should provide supporting documentation in sufficient detail to permit a complete evaluation of the proposal. The Government may conduct a crosswalk between the information provided in offerors proposal volumes to assess whether the offeror submits consistent proposal information.

L.6.4 Single Proposal Submission: Offerors are limited to submitting one proposal with one approach to meeting the requirements of this solicitation. An offeror is defined as the party that makes an OFFER and looks for acceptance from the offeree [Black's Law Dictionary, page 1190 (9th ed. 2009)]. An entity competing independently cannot share a common parent, cannot have a parent/subsidiary relationship with any other offeror, and it cannot be affiliated with any other offeror.

L.6.5 All or None: Offers in response to this solicitation must be submitted for all the requirements identified in the solicitation. Offers submitted for less than all the requirements call for by this solicitation may be rejected or ineligible for award.

L.7 PROPOSAL DOCUMENTS

L.7.1 Proposals shall be clear and concise and include sufficient detail for effective evaluation. The offeror should not simply rephrase or restate the Government's requirements, but rather shall provide convincing rationale to address how the offeror intends to meet those requirements. The offeror should assume the Government has no prior knowledge of its capabilities and experience. The Government will base its evaluation on the information presented in the offeror's proposal in response to this solicitation.

L.7.2 Proposals are to be structured in accordance with the CLIN structure set forth in Section B.

L.7.3 The offeror's response to this solicitation shall consist of the following:

- 1) Proposal Summary, Volume 1
- 2) Technical Proposal, Volume 2
- 3) Past Performance, Volume 3
- 4) Price Proposal, Volume 4

L.7.4 The PROPOSAL SUMMARY, Volume 1, shall include:

- Solicitation Number
- Date Submitted
- Offeror's Name
- Offeror's Contract Manager Contact Information
- Offeror's CAGE Code and UEI Number
- All proposed subcontractor(s) (as applicable)
- Proposal Validity Date
- OCI Plan or Negative Affirmation (PWS 1.6.12 and L.8.1.1)
- Quality Control Plan (PWS 1.6.1)

L.7.4.1 IAW Section L.5.3, the offeror shall specify a period of not less than 120 days from date of closing. This date may be extended by mutual agreement.

L.7.4.2 Quality Control Plan (PWS 1.6.1): The offeror shall submit a draft Quality Control Plan with their proposal which articulates their proposed approach for maintaining quality control that is integrated

into the overall management approach and meets the requirements of the PWS. The QCP is a part of the proposal summary volume. There is no page limit. The Quality Control Plan will not be evaluated as part of the Best Value Tradeoff.

L.7.5 The TECHNICAL Volume, Volume 2, shall include:

The Technical Volume, consisting of the offeror's Technical Knowledge and Staffing (Surge Capacity and Qualifications of the Offeror's Personnel), will present relevant information articulating the offeror's proposed approach to meeting the technical and staffing requirements and objectives of the Office of the Chief Financial Officer (OCFO) Remediation requirement. The volume should clearly demonstrate the offeror's understanding by providing a clear description of the proposed approach to performing the work. The offeror's description should include a clear description of all processes and procedures employed. Offerors should provide relevant experience (for this purpose, experience refers to what an offeror has done, not how well it was accomplished) in performing proposed process and procedures. This volume shall not include any cost or pricing data. The offeror's proposal information submitted will be evaluated to assess the risk that the offeror will timely meet contract requirements. Each technical subfactor is equal in importance.

L.7.5.1 Technical Knowledge

L.7.5.1.1 The contractor shall provide a clear and detailed approach to meeting the Government's objective and executing all PWS requirements. The contractor's technical approach shall demonstrate the ability to meet various project timelines, ability in delivering products timely, and the ability to successfully achieve the Government's desired outcome of this requirement. The contractor must demonstrate industry-proven practices and processes that it will be used to achieve the Government's desired outcome. The contractor shall also demonstrate sufficient and detailed evidence which demonstrates mastery, capability, and capacity to deliver each of the tasks specified under Paragraph 1.4 and Part 5 of the PWS. Finally, the contractor shall demonstrate its detailed knowledge and expertise in remediation support of internal controls and audit findings. Specifically, the contractor must show expertise in remediating business process findings to ensure compliance with GAO Green Book Standards, testing remediation efforts to validate compliance with GAO Green Book Standards, and remediating IT control findings and related risks to ensure compliance with GAO Green Book Standards.

L.7.5.1.2 The offeror shall also provide a management approach that explicitly defines and details the offeror's capability to successfully manage, perform, and execute the Government's requirement. The contractor shall delineate its organization's resources, tools, and systems, and provide high level project management and quality control for this contract. The offeror shall provide a draft Quality Control Plan that demonstrates how quality, as outlined in the PWS's performance standards in the Performance Requirements Summary (PRS) will be met or exceeded. The offeror must provide performance measures in addition to those stated in the PWS that are clear, meaningful, measurable, challenging, and show the offeror's ability to meet the objectives identified within the PWS.

L.7.5.2 Staffing, Surge Capacity and Qualifications of the Offeror's Proposal

L.7.5.2.1 The contractor shall describe its staffing plan to ensure a stable and qualified workforce over the life of the contract by detailing its ability and approach to recruiting and retaining qualified personnel as outlined in the bullets below:

L.7.5.2.1.1 Methodology by which the contractor plans to maintain an environment in which highly skilled and qualified people will make long-term commitments to achieving the Government's mission. Highly skilled and qualified people is defined as personnel that have the expertise required to perform the specific tasks areas as defined in the PWS;

L.7.5.2.1.2 Demonstrate the number of employees, labor mix, as well as knowledge and skills of employees that can successfully deliver the studies and analyses required to meet the Government's requirements;

L.7.5.2.1.3 The ability to provide potential surge of staff and the necessary oversight to address any internal control failures that could have a negative impact on the DHS and FEMA internal control environment.

L.7.5.2.1.4 The offeror shall provide a narrative describing how qualified personnel will be provided, as required in the OCFO Remediation requirements and deliverable requirements through a qualified workforce meeting requirements of the estimated workload of an estimated 30,000 hours per year (these hours do not include surge possibilities) over the five-year ordering period for this BPA. The offeror shall describe its overall staffing and recruiting process utilized to attract, retain, and maintain qualified personnel at optimal staffing levels to accomplish call order requirements over the life of the agreement, to include meeting possible future increases in required level of effort. The offeror shall describe its use of labor sources to attract qualified candidates and its plan to ensure these candidates meet the minimum qualifications (experience level, education, background, and possible clearance) required for each labor category description in the PWS. The offeror shall describe its experience with an historical ability to recruit and retain personnel and how this capability will be utilized to successfully meet the requirements of this PWS.

L.7.5.2.1.5 The offeror shall specifically identify and substantiate its staffing processes to meet the staffing requirements of the OCFO Remediation requirement.

L.7.5.2.1.6 The offeror shall describe its proposed approach to ensure continuity of Remediation services, without interruption, when a contractor employee is off for any reason.

L.7.5.2.1.7 Offerors shall submit a Technical Staffing Matrix with their technical volume. The Technical Staffing Matrix must identify each of the proposed labor categories (key personnel, auditor, etc.).

L.7.5.2.2 The contractor shall submit resumes of required Key Personnel with signed commitment statements for each (the signed commitment statement shall not exceed two pages) of the Key Personnel listed in Section 1.6.8 of the PWS. The resumes shall demonstrate the technical competency of the proposed Key Personnel to support the requirement of the scope by describing specific, relevant experience, and skillsets of Key Personnel in providing services described in the PWS.

L.7.5.2.2.1 For all Key Personnel (PWS 1.6.8 and Table in Part 6) who will be employed in the Management of the OCFO's BPA, offerors shall include information regarding the authority and levels of responsibility of the key personnel with respect to staffing, technical performance, schedule, deliverables, quality, and decision making.

L.7.5.2.2.2 Key Personnel Resume(s): Key personnel are those persons (or is the person), whether employed by the offeror or a subcontractor (if applicable), who will occupy any key personnel position(s) for the Agreement as identified in the offeror's proposal. The offeror shall submit resumes for key personnel proposed. Each resume is limited to three pages and shall include:

- Proposed Key Personnel position
- Planned duration of the assignment
- Current Assignment: Position presently occupied, to include title and organization and employer
- Availability / Allocation: Relationship to the offeror (full/part-time, prime contractor employee / subcontractor employee), Percentage of time to be committed. Letter of Commitment shall be provided for all key personnel (such letters shall be signed by both the employee and the appropriate representative of the contractor). Submission of resumes of individuals not currently employed by or with whom the contractor does not have a bona fide employment contract (contingency resumes) shall also provide a phase in plan showing the availability of the qualified personnel and length of time required to reach full support. Contingency resumes shall include a Letter of Commitment signed by the individual being proposed that clearly states their commitment to enter into employment with the contractor and the proposed salary.
- Education: Degree, school, majors
- Relevant Qualifications and Specialties: A brief summary of training, qualifications, achievements,

honors, awards, publications, and professional organizations

- Employment History and Experience: A list showing the programs on which the individual has worked, the highest position held on each program and the duration (including the starting and ending dates) of assignment to each program

L.7.6 The PAST PERFORMANCE Volume, shall include one of the following or a mix of the three:

L.7.6.1 Offerors shall list at least three, but not more than five, clients familiar with performance (include name, telephone number, physical address, and email address), and provide a short description of the work performed.

L.7.6.1.1 List three projects completed within the past five-years, with either the Federal Government or commercial customers, which demonstrate work similar in type to the work described in this solicitation. The offeror's past performance must be in the role as the prime contractor.

L.7.6.1.2 List contract and/or task order reference number, contract and/or task order annual and total dollar value, contract and/or task order period of performance, and role performed – including whether the offeror acted as the prime or subcontractor.

L.7.6.2 Offerors can submit assessments out of the CPARS system that includes the contract number, the period of performance, and the amount of the contract. These reports should not be older than three years from this proposal due date. Any pages over the 15-page limit will not be evaluated.

L.7.6.3 Offerors can submit the portion of the Past Performance Questionnaire (PPQ) offerors are to complete and forward to previous customers. These documents will not be counted against the offeror's 15-page limit, because when the document is forwarded to FEMA from the assessor, those pages will be included.

L.7.7 The PRICE Volume, shall include:

L.7.7.1 Price Proposal Format: Electronic spreadsheet files (Workbooks) shall be sent in MS Office 365 compatible format, and include all formulas, functions, macros, computations, or equations used to compute the proposal amounts. There can be no cell references to data or files which are not included in the Price Volume.

L.7.7.1.1 Table of Contents: The offeror and each subcontractor (if applicable) shall provide a Table of Contents showing each file submitted as part of the Price Volume with a short description of the contents of the file. Each of these entries in the Table of Contents shall be hyperlinked to the representative files.

L.7.7.1.2 Price Proposal Spreadsheet: The offeror shall submit all proposed prices utilizing the Governments Price Proposal Spreadsheet (Section J and will be submitted with RFP). The attachment shall be completed in accordance with the instructions provided in the attachment. No other format will be accepted.

L.7.7.1.3 The offeror shall only submit proposed prices in Volume 4. No price data shall be included in any other volume.

L.7.7.2 Price Information: The offeror shall submit pricing data substantiating the price proposed to complete the requirements identified in the RFP PWS. The offeror's price proposal shall contain sufficient factual information to establish the fair, reasonableness, and completeness of the proposed price.

L.7.7.2.1 The submitted price information and data shall include at least the following:

L.7.7.2.1.1 A narrative on the basis of estimate (BOE), by element.

L.7.7.2.1.2 A narrative description of the tasks to be performed.

L.7.7.2.1.3 A description of each administrative and management labor category used in the BOE.

L.7.7.2.2 Cost Decrements: In the event the proposed prices are calculated using any form of price decrement (to include price discounting, expected negotiation decreases, corporate investment, or management challenges), the offeror shall identify such decrements in the proposal. Where price decrements are proposed, identify the nature, amount, and basis for the decrement, and any accounting treatment implications.

L.7.7.2.3 Past Experience-Based Estimates: Where price estimates are based on past experience (historical data), identify the past experience, explain how the past experience relates to the current effort, including similarities and differences, and how price data available from the past experiences were adapted to the current effort.

L.8 ORGANIZATIONAL CONFLICT OF INTEREST

L.8.1 All offerors shall make a preliminary disclosure to the Contracting Officer, at the time of its proposal, of any Organizational Conflict of Interest issues it has identified. An offeror failing to submit an OCI plan that is later determined should have been submitted, could cause the proposal to be rejected and no longer be considered for award. Offerors shall include in its plan where its employees are located and the total number of employees in the location(s).

L.8.1.1 Offerors without any Organizational Conflict of Interest issues shall include a statement (negative affirmation) of this in the proposal.

L.8.2 Organizational Conflict of Interest (OCI) – Definition: OCI means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage [FAR 2.101]. An OCI may result when factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the instant contract creates an actual or potential conflict of interest on a future acquisition. In the latter case, some restrictions on future activities of the contractor may be required [FAR 9.502(c)].

L.8.3 The provisions of FAR 9.5, Organizational Conflict of Interest, apply to any award made for the OCFO Remediation Requirement. Potential offerors should review their current and planned participation in any other Government contracts, subcontracts, consulting, or teaming arrangements where they may be in a position of actual or perceived bias or unfair competitive advantage. A common example with the potential for OCI is where an entity performs work both as a system contractor/subcontractor and as a Government support contractor for Government offices involved in the FEMA supporting program efforts or related programs.

L.8.4 Offerors should disclose any potential OCI situations to the Procuring Contracting Officer (PCO) as soon as identified including prior to proposal submission. The disclosure should include the facts and an analysis of the actual or perceived conflict and a recommended approach(es) to neutralize or mitigate the potential conflict. The preferred approach to potential conflicts is to negate/obviate the conflict. Mitigation is considered only if it is not practical to negate/obviate the conflict. The PCO will promptly respond to resolve any potential conflicts.

L.8.5 The PCO will review the proposed plan, but this submission will not be evaluated as part of the source selection decision.

L.8.5.1 The plan or negative affirmation (L.8.1.1) shall be included in Volume 1 of the offeror's proposal.

52.204-7 System for Award Management. (OCT 2018)

52.204-16 Commercial and Government Entity Code Reporting. (AUG 2020)

52.233-2 Service of Protest. (SEP 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from Shawn Smith/
shawn.smith@fema.dhs.gov.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

M - Evaluation Factors for Award

SECTION M: EVALUATION FACTORS FOR AWARD

M.1 BASIS FOR BLANKET PURCHASE AGREEMENT (BPA) AWARD

M.1.1 The Government intends to award a single Hybrid Firm Fixed Price (FFP) and Labor Hour (LH) Blanket Purchase Agreement (BPA) as a result of this Request for Proposal (RFP), but reserves the right to make no award, if it is determined to be in its best interest. The BPA awarded will be made on the basis of Best Value for the Government. Evaluation factors are listed in descending order of importance. All evaluation factors other than cost, when combined, are significantly more important than price. The award will be made to the responsible offeror whose proposal represents the best value to the Government.

M.2 DETERMINATION OF CONTRACTOR RESPONSIBILITY AND ELIGIBILITY FOR AWARD

M.2.1 Per FAR 9.103, Agreements will be placed only with an offeror that the Contracting Officer determines to be responsible, that is, those who can satisfactorily perform the necessary tasks and deliver the required services on time. Prospective offerors, in order to qualify as sources for this acquisition, must be able to demonstrate they meet standards of responsibility set forth in FAR 9.104. In addition, the Government may assess the offeror's financial ability to meet the RFP requirements. The Government reserves the right to conduct a Pre-Award Survey on any or all offerors to aid the Procuring Contracting Officer (PCO) in the evaluation of each offeror's proposal and ensure that a selected offeror is responsible. No award can be made to an offeror who has been determined to be not responsible by the Contracting Officer.

M.3 REJECTION OF OFFERS

M.3.1 Offerors shall carefully read, understand, and provide all the information requested in the Proposal Preparation Instructions contained in Section L. If there are any parts of Section L instructions the offeror does not understand, the offeror may request clarification from the Contracting Officer in writing before the closing date of the solicitation. In accordance with FAR 52.215-1, contained in this RFP, the Government may reject any or all proposals if such action is in the Government's interest. Examples include, but are not limited to, the following:

M.3.1.1 The proposal fails to meaningfully respond to the Proposal Preparation Instructions specified in Section L of this solicitation. Examples of failure to meaningfully respond include:

- i. When a proposal merely offers to perform work according to the RFP terms, or fails to present more than a statement indicating its capability to comply with the RFP terms, or does not provide support and details as specified in Section L of this solicitation.
- ii. When a proposal fails to provide any of the data or information required in Section L.

iii. When an offeror's proposal provides some data and information but omits significant material data and information required by Section L.

iv. When a proposal merely repeats Performance Work Statement (PWS) without elaboration.

M.3.1.2 The Government may reject any offeror's proposal that is unbalanced as to cost. In accordance with FAR 15.404-1(g), an unbalanced offer is one which is based on prices significantly high or low for one given period versus another period. There must be a direct relationship between the effort expended and its price for each tasking.

M.3.1.3 The Government may reject any offeror's proposal that offers a product or service that does not meet all stated material requirements of the solicitation.

M.4 EVALUATION AND SOURCE SELECTION PROCESS

M.4.1 Evaluation Process: Proposals will be evaluated using a "trade-off" process to obtain the best value to the Government. As part of the best value determination, the relative strengths, weaknesses, and risks of each proposal shall be considered in selecting the offer that is most advantageous and represents the best overall value to the Government. The Government may make no award where it concludes that no proposal exists with a reasonable probability of achieving program and contract terms and conditions at an acceptable level of risk or cost.

M.4.2 Source Selection Authority: The Source Selection Authority (SSA) is the official designated to direct the source selection process and select the offeror for BPA award.

M.4.3 Source Selection Evaluation Board (SSEB): An SSEB has been established by the Government to evaluate proposals in response to this solicitation. The SSEB is comprised of technically qualified individuals who have been selected to conduct this evaluation in accordance with the Evaluation Criteria for this solicitation. Careful, full and impartial consideration will be given to all proposals received pursuant to this solicitation, as well as the evaluation of such proposals.

M.4.4 Discussions: The Government intends to evaluate proposals and make award without discussions. The Government reserves the right to later determine to hold discussions in accordance with FAR Clause 52.215-1 Alternate I.

M.4.5 Importance of Price: All the factors contained in each proposal will be evaluated. However, the closer the offeror's evaluations are in the non-cost factors, the more important the cost becomes in the decision. Notwithstanding the relative order of importance of the Evaluation Areas as stated in Section M herein, Price may be controlling when:

M.4.5.1 Proposals are otherwise considered approximately equal non-price areas; or

M.4.5.2 The advantages of a higher rated, higher cost proposal are not considered to be worth the cost premium

M.4.6 The evaluation of proposals submitted in response to this solicitation, and source selection, shall be conducted using a tradeoff process to obtain the best valued proposals to the Government. Proposals which are eligible for award will be subject to the Source Selection Tradeoff process, considering both the Evaluation Factors and their relative order of importance as cited in M.5.1, to identify the proposals which represents best values for the Government. As part of the best value determination, in selecting the offers that is advantageous and represents best values to the Government, the relative strengths, weaknesses, and risks of each offeror's proposal will be considered, as specified below, in addition to the other evaluation methods described below. Selection of the successful offeror shall be made following an assessment of each proposal, based on the responses to the information requested in Section L of this solicitation and against the solicitation requirements and the evaluation criteria described in Section M.

M.4.7 Consistency: The Government may conduct a crosswalk between the offeror's proposal volumes to assess whether the offeror submits consistent proposal information as required in Section L. Any inconsistency between proposal volumes, which indicates the offeror has an inherent misunderstanding of the requirements or an inability to perform the resultant contract, may result in an offeror being determined ineligible for award or being assessed with increased risk in the Technical Factor.

M.5 SOURCE SELECTION EVALUATION FACTORS

The Government will assess each offeror in four factors: (1) Technical Knowledge; (2) Staffing, Surge Capacity and Qualifications of the Offeror's Personnel (3) Past Performance; and, (4) Price. Best value will be determined based on the following weighted factors in descending order of importance: Technical Knowledge; Staffing, Surge Capacity and Qualifications of the Offeror's Personnel; Past Performance; and, Price.

M.5.1 The Government intends to award a BPA using a Best Value tradeoff process as the basis for award. A rating of Unacceptable or Marginal in Factors 1 or 2 will render the entire proposal technically unacceptable, and therefore, not eligible for award. Factor 1 is more important than Factor 2 through 4. Factor 2 is more important than Factor 3. And, Factor 3 is more important than Factor 4. All evaluations factors, other than cost or price, when combined, are significantly more important than price.

M.5.2 TECHNICAL KNOWLEDGE FACTOR

M.5.2.1. The Government will evaluate the technical approach based on the contractor's ability to: 1) Demonstrate a clear understanding of the work to be performed; 2) Demonstrate the methodology and plan to successfully meet or exceed the Government's objectives; and, 3) Demonstrate its expertise and knowledge required to successfully perform the requirements of the PWS.

M.5.2.2. The Government will evaluate the management approach based on: 1) The extent to which the contractor demonstrates capabilities to successfully manage, perform, and execute the PWS requirements; and, 2) The contractor's Quality Control Plan and how well the plan demonstrates oversight and how quality standards, as outlined in the Performance Requirements Summary, will be achieved and maintained during performance.

M.5.3. STAFFING, SURGE CAPACITY AND QUALIFICATIONS OF THE OFFEROR'S PROPOSAL

The Government will evaluate the offeror's proposed personnel's qualifications, relevant experience, and technical expertise. The Government will consider the extent to which the offeror's number of employees, labor mix, as well as knowledge and skills of contractor staff can successfully complete the remediations required under this requirement. The Government will evaluate the offeror's capability to provide potential surge of staff and the necessary oversight to address any internal control failures that could have a negative impact on the DHS or FEMA internal control environment. Additionally, the Government will evaluate resumes for key personnel expected to provide services for this requirement. Therefore, the offeror shall provide key personnel resumes with a signed commitment statement for each of the key personnel (the signed commitment statement shall not exceed two pages) for the following labor categories:

Senior IT Security Consultant (Key)
Senior Manager (Key)
Audit Senior Management Level III (Key)
Information Technology Specialist
Staff II
Senior
Manager

Audit Senior Project Support III
Audit Project Support – V
Audit Lead III (Key)

M.5.4. PAST PERFORMANCE

M.5.4.1. The Government will evaluate information regarding past performance performing services that are relevant to the requirements of the RFP. Relevant services are those that have been completed or are currently in process, which are of similar size, dollar value, scope, and complexity to the services required by this RFP, and that were provided within five years preceding the closing date of this RFP. Past performance information may include those provided to the federal Government, state and local Government agencies, and commercial customers. If the offeror does not possess any relevant past performance, then the offeror shall submit a statement affirming such. In the event the offeror possesses no relevant past performance, the offeror will be given a neutral rating.

M.5.4.2. The Government may at its discretion, evaluate and consider other relevant past performance information to which it has access, such as the Contract Performance Assessment Reporting System (CPARS) and may contact references for any information that comes into its possession. Offerors must provide the following past performance information:

M.5.4.3. Offeror's past performance will be evaluated on the similarity size, complexity, dollar value, and contract type. The offeror's past performance will be further evaluated based on the offeror's reputation for timely, accurate, and cooperative performance, as well as information obtained from all available sources. The Government will place greater value on verifiable experience, such as examples, that are similar or the same as the requirements in the PWS.

M.5.5 PRICE

M.5.5.1. BPA Call Orders placed against resulting awarded BPA will be either Labor Hour (LH) or Firm-Fixed Price (FFP) with a definite goal or target specifying an end product. These will not be term contract vehicles where the contractor's obligation is stated in terms of a specified level of effort for a stated period of time.

M.5.5.2. The Government will evaluate price reasonableness in accordance with FAR 15.404-1. The Government shall evaluate the reasonableness of the offeror's proposed price in accordance with FAR 31.201-3. A cost is reasonable if, in its nature and amount, it does not exceed that which would be incurred by a prudent person in the conduct of competitive business.

M.5.5.3. Evaluation of Options will be conducted in accordance with FAR 52.217-5, Evaluation of Options, to include FAR 52.217-8, Option to Extend Services, and FAR 52.217-9, Option to Extend the Term of the Contract. Evaluation of options shall not obligate the Government to exercise any options. The objective of the evaluation of options is to determine the cost of each of the options to be fair and reasonable at the time of award of the resulting BPA. Unrealistically low, high, or unbalanced pricing options in the proposal may be considered a performance risk. The evaluations will apply to BPA calls, because the BPA will be awarded with a five-year ordering period.

M.5.5.4 The price evaluation factor is significantly less important than the non-cost factors.