STATEMENT OF WORK FOR
Office of National Continuity Programs (ONCP)
Business Management Division (BMD), Program Management Support

Date: March 03, 2023

1. PURPOSE

The Office of National Continuity Programs (ONCP) mission is to coordinate the implementation of Executive Branch continuity plans and programs and will guide and assist the continuity planning efforts of both government and non-government stakeholders in order to sustain the continuous performance of National Essential Functions. Furthermore, ONCP serves the public by preserving our Nation's constitutional form of government across a wide range of potential threats and emergencies. On behalf of the Secretary of Homeland Security and the FEMA Administrator, ONCP coordinates the planning, implementation, and execution of executive branch continuity programs in support of National Essential Function (NEF) 1, preservation of our Constitutional Government.

2. BACKGROUND

ONCP recently went through a realignment within the Program Management Office (PMO) of which new divisions were enhanced by assigning new responsibilities and executing strategic priorities accordingly. The Business Management Division (BMD) falls under one of those divisions. The role of BMD is to provide timely, cost-effective, and critical business reporting in support of key division stakeholders in BMD's five major areas of responsibility. Those areas of responsibility are as follows: 1) Budget and Financial Management, 2) Acquisitions Management, 3) Human Resources Administration, 4) Asset Management, and 5) Portfolio Oversight.

BMD personnel will proactively support ONCP activities, to include: 1) facilitating, managing, and continuously improving appropriate information flow among and between all division stakeholders; 2) acting as senior business advisors to increase efficiency and effectiveness; and 3) concurrently maintaining and improving customer relationships management activities with division stakeholders.

3. SCOPE OF WORK

a. Portfolio Oversight

BMD is responsible for supporting investment programs as part of the PMO effort to ensure effective and efficient program execution and is responsible for program governance and acquisition policy. BMD will assist ONCP components in building the PMO's acquisition

and program/project management capabilities. The division will also assist and serve as advisors for managing the health of acquisitions and investments within ONCP. Contract support that pertains to these functions are as follows:

1. Assist in developing and updating program management policies, process, and workflows
2. Assist in supporting BMD's effort of balancing the interests of the division through efficiency, accountability, and effectiveness
3. Develop best practices to assist in guiding and supporting ONCP/BMD through development, production, deployment, operations, support, and disposal of projects/programs
4. Assist in providing objective technical analyses of programs/projects and portfolios to support decision makers and manage program reporting

b. Project Management Support

FEMA ONCP BMD requires Contractor support to provide the full suite of project management deliverables and associated activities. Support includes expertise in program/project areas relevant to acquisition, budget, human resources, logistics, and portfolio management. Contractor shall provide direct project management support and shall hold a current Project Management Professional (PMP) certification. Types of work included but are not limited to areas such as developing, maintaining, and updating an integrated master schedule, and assisting in the drafting of strategic plans, governance documents, standard operating procedures (SOPs), project charters, quality assurance, and other documents related to managing BMD programs. Support for project management may include but not be limited to the following activities:

1. Program Integration: The Contractor shall assist in project specific deliverables which include:

   a. Assist in drafting, monitoring, and updating project management plans
   b. Assist in developing and delivering project specific education and communication
   c. Assist in monitoring and controlling project specific work
   d. Assist in configuration management
   e. Assist in linking performance measurement across BMD
   f. Assist in designing and monitoring compliance with quality assurance and internal control procedure
   g. Assist in developing a risk management plan for BMD programs as a whole and risk-management plans for individual projects
   h. Assist in documenting the scope of individual projects within BMD to include:

i. Filing and recording BMD architectural documentation
ii. Filing and communicating a description of BMD
iii. Assisting in writing scope statements for individual projects

2. Schedule: ONCP/BMD is comprised of multiple projects; each having a schedule of deliverables with multiple stakeholders. Some deliverables have high visibility with ONCP and FEMA senior leadership. Contractor shall assist in an integrated schedule of BMD projects and providing monthly updates to BMD management.

c. Communication Support

The Contractor shall assist with multiple types of communication support to include:

1. Assist in setting up standard reporting templates for projects.

2. Assist the Director of BMD with calendar management support

3. Assist with project status meetings, to include the following tasks:

a. Developing a schedule for status meetings
b. Developing meeting agendas
c. Assisting in coordinating BMD All Hands meetings (Contractor shall take notes during such meetings and develop an action item list that will be required to be forwarded to all participants of those meetings)

4. Assist in developing Power Point presentation slides

5. Assist in collecting and analyzing input from multiple participants during meetings to include the following:

a. Assist in providing written reports, analysis, and assessments of projects. Assist with the completion of acquisition, budget, human resources, logistic, and portfolio management documentation
b. Assist in developing required briefings for key non-technical experts including senior leadership
c. Support ongoing activities and interactions between BMD and its stakeholders. The program management task will cover support for programmatic, working-level meetings for specific projects within BMD

d. Financial Management Branch (FMB)

FMB was formed to support the ONCP Directorate and to ensure all ONCP finances are managed in an efficient and effective manner to accomplish the ONCP mission. BMD requires support in the coordination, reporting, and tracking of the executed budget to

enable ONCP to meet regulatory and statutory obligations. In addition, DHS, FEMA senior leadership, and the FEMA Office of the Chief Financial Officer (OCFO) conduct various reviews of executed budget to ensure compliance. FMB requires assistance with gathering data and ensuring the accuracy of the data presented in these reviews to include the following specific requirements:

1. Assist in developing manageable budget milestones aligning with FEMA and DHS goals. Milestones shall be aligned with DHS-wide earned value management (EVM) guidelines related to cost accounting and financial management
2. Assist in budget formulation and execution, with analysts supporting division portfolios
3. Assist in Event Tracking and Approval (ETA) and Travel Submission Management
4. Aid in package review, approval, and email through Enterprise Coordination Approvals Processing System (ECAPS) tracking and approval
5. Provides support for developing status of funds and briefing charts
6. Assists in preparing required OCFO quarterly and annual Undelivered Order Obligation (UDO) reconciliation requirements
7. File and store all documentation according to the FMB configuration management plan and file record system
8. Assist in creating, processing, and following through on financial documentation for knowledge management and auditing authorities

9. The Contractor shall assist in the creation of FMB-related PowerPoint presentations (*proficient in all Microsoft Software applications) (Senior Level preferred).

e. Acquisition Management Branch (ACMB)

ACMB requires Contractor support in drafting and processing required documents for acquisition program review by ONCP and FEMA senior executives. The Contractor must have a Project Management Professional (PMP) certification to support this particular branch. There are specific mandatory documents for DHS programs to meet specified criteria. All documents must be in compliance with DHS timelines for updates, which may vary for different documents. The Contractor shall assist with the following:

1. The Contractor shall be knowledgeable of the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), the Anti-Deficiency Act (ADA), Information Technology Acquisition Review (ITAR), Federal Information Security Modernization Act of 2014 (FISMA), Federal Information Technology Acquisition Reform Act (FITARA), the Planning, Programming, Budgeting & Execution Process (PPBE), Defense Production Act (DPA), intellectual property laws and rights, Freedom of Information Act (FOIA), and Office of Management Budget (OMB) policies and guidance.
2. The Contractor shall assist with the determination of what supplies or services are to be acquired by the Government (as an agency may give contractors authority to

acquire supplies at prices within specified ranges and subject to other reasonable conditions deemed appropriate by the agency);

3. The Contractor shall assist BMD and other program offices within ONCP with defining requirements and identifying specifications.
4. The Contractor shall assist with conducting market research, developing inputs for government cost estimates, drafting statements of work and other pre-award documents, and preparing technical evaluation and associated documentation,
5. During the pre-award phase, the Contractor shall assist with the determination that prices and labor rates are fair and reasonable.
6. The Contractor shall assist with the contract close-out process and the post-award phase.
7. The Contractor shall support the reconciliation process of ensuring that Contract Line-Item Number (CLIN) cumulative balances corresponds to the financial reports submitted by contractors and vendors.
8. The Contractor shall assist with the review and determination of payment for vendor invoices for existing, awarded contracts.
9. The Contractor shall manage the BMD/ACMB relational database, including data entry and generation of database reports as directed with updated contract data and information.
10. The Contractor shall assist with the migration and transferring of contract data and information from the Acquisition Portfolio Matrixes (APMs) to Tableau (a Salesforce company).
11. The Contractor shall coordinate with DHS/FEMA, other federal agencies, FEMA regions, and other partners to identify and gain access to contract reporting, datasets, and other resources relevant to acquisitions and procurements.
12. The Contractor shall support the integration of new data into Tableau.
13. The Contractor shall update the APMs prior to the migration of contract data and information into Tableau. Conduct corrective action entries based on information collected from vendors and key stakeholders and partners within ONCP, FEMA, DHS, and other federal agencies.
14. For data analysis, the Contractor shall conduct open-source research and basic qualitative analysis of ONCP's contract data and information and interagency data to identify trends in acquisitions and procurements.
15. The Contractor shall support the categorization of information based on established qualitative assessment methodology and basic statistical analysis of acquisitions and procurement data and information.
16. The Contractor shall support advanced quantitative and qualitative analysis of ONCP's contract data and information.
17. For data reporting, deliverables shall include the development of reporting templates for recurring acquisitions and procurement products, including Tableau reports,

visualizations of dataset analyses, ad hoc, and annual analyses of contractual dataset.

18. The Contractor shall provide advanced analytic support to ONCP senior leadership on ad hoc consultancy basis.
19. For data integration and management, the Contractor shall aid with the development of database management approach for BMD and the revision of existing BMD methodologies and/or development of new methodologies for integrating new datasets into acquisitions and procurement products.
20. The Contractor shall assist with the development, the facilitation, and updating of new Business Process Improvements (BPI). The Contractor shall develop and update Analysis of Alternatives for various projects.
21. The Contractor shall develop and update Lifecycle Cost Estimates (LCCEs) for various projects and programs within ONCP.
22. The Contractor shall develop new acquisitions, procurement, and programmatic documentation required by FEMA or DHS.
23. The Contractor shall assist ONCP's Action Office and the Office of the Associate Administrator (OAA), as required.
24. The Contractor shall assist in writing documents that pertain to all technical areas (i.e., requirements development, acquisitions, systems engineering, logistics, business case development, etc.).
25. The Contractor shall assist in maintaining and updating ONCP website.
26. The Contractor shall assist with SharePoint management documentation and all other relations to SharePoint within BMD.
27. The Contractor shall assist in the creation of ACMB-related PowerPoint presentations (*proficient in all Microsoft Software applications) (Senior Level preferred).

f. Assets Management Branch Support

1. The Asset Management Branch (AMB) requires assistance in the inventory and tracking of ONCP/ BMD property to include government-furnished property (GFP) and contractor-acquired property (CAP). Also, ONCP requires assistance in developing, implementing, and improving processes to ensure ONCP property is accountable, as well as complying with Government property management regulations and directives governing the acquisition, use, and disposal of Personal Property maintained in the Sunflower Asset Management System (SAMS).

a. Thoroughly understand the Personal Property FEMA Manual 119-7-1 which is to be used in managing and accounting for Government property controlled by FEMA.
b. Thoroughly understand the Sunflower Asset Management System (SAMS) Navigation Guides Asset Transactions which is to track assets from acquisition through disposal.

1. Generate reports from SAMS throughout the inventory period to assess the progress of the inventory.
2. Verify the accuracy of all records for their accountable areas.
3. Immediately report any issues that may alter the outcome, success, or timing of the inventory period.
4. Perform all SAMS administrative actions.

c. Monitor the storage, utilization, transfer, and disposal of Personal Property through close coordination with the APO and maintain a record of all such transactions.

d. When Personal Property has been reported lost, stolen, damaged, misused, or destroyed, prepare a FEMA Form 119-7-1-1, Report of Survey, and forward all required and pertinent documentation.

e. Be familiar with the FEMA Fleet Management Manual 119-24-1 which is to provide guidance and clarity relative to daily fleet management operations.

1. Conduct inventories at all levels (cyclic and/or annually) to verify the existence, location, and quantity of personal property and keep track of property in accordance with the FEMA manual and the SAMS guide. Some tasks may require lifting of equipment of up to 50 lbs.
2. Assist in reconciling discrepancies between the official FEMA property system and ONCP procurement records, custody receipts, and internal spreadsheets and databases. This requirement will include internal and external stakeholders.
3. Assist AMB government property custodians with ensuring that all contractors and government employees comply with all agency policies regarding property accountability.
4. Be available to travel within a three-day notice to assist in the preparation of a cyclic or annual inventory of FEMA-owned property at FEMA Regional Offices, State Emergency Operations Centers, and US Territories.
5. Assist with perform market research to determine the appropriate requirements document for an acquisition according to AMB circumstances.
6. Provide administrative support with PowerPoint presentations related to AMB and logistics support with the distribution of new FEMA-owned and disposition of old equipment after its "useful life."
7. In the performance of this requirement, the Contractor may be required to operate FEMA vehicles such as passenger cars or box trucks. If tasked to operate government-owned vehicles, the contractor will be held liable for any costs associated with misuse of Agency vehicles and must provide proof of liability insurance coverage. Additionally, the contractor must obtain prior approval from the Contracting Officer Representative (COR) to use Agency

vehicles, and must restrict their use to official purposes, only in performance of this contract.

g. Human Resources Administration Support

1. The Contractor shall assist in project specific deliverables which include but are not limited to:

    a. Monitor and update HRA's and BMD's quarterly project management BMD branch plans for the Director of BMD's Individual Performance Review (IPR) and ONCP Executive Management

    b. Assist in developing, maintaining, and delivering project specific HRA education and communication (i.e., Employee Orientation Workshop, Employee Handbook, ONCP newsletter, Professional development emails)

    c. Assist in monitoring, updating, and controlling Deployment Rosters, Cascade SOP, ONCP Personnel Contact list, and any other related ONCP roster

    d. Assist in monitoring, updating, and controlling Training SOP, and any other related Human Resources related SOPs

    e. Assist in creation of Human Resources related PowerPoint presentations (*proficient in all Microsoft Software applications) (Senior Level preferred).

    f. Assist in the project management for various HRA activities to include developing SOPs that describe various HRA processes as described and managing calendar of projects.

    g. Assist in proofreading and providing feedback for all Human Resource- related correspondence packages prior to the BMD Director signing their concurrence

    h. Assisting with HRA project status meetings, to include the following tasks:

        1. Developing a schedule for a status meeting.
        2. Developing meeting agendas.
        3. Facilitating meetings.

2. The contractor shall assist in all aspects of HR work that fall outside of FedHR, PAL, Tableau, webTA, and other electronic systems. The contractor shall assist with the following activities:

    a. Holding pre-recruitment consultations with hiring managers;
    b. Drafting recruitment forms (to include developing ideal candidate statements, duties summaries, job analyses, and weighing plans);
    c. Developing positions descriptions;
    d. Producing weekly vacancy update reports; and
    e. Maintaining/updating org charts.

3. Additional Details

a. Provides a detailed look into ONCP-BM strengths and weaknesses, which helps management make necessary changes to improve productivity within.
b. Develops and plans strategic recruitment methods to advise management on the effectiveness of program operations and resource utilization.
c. Prepares recruitment packages, reviews draft vacancy announcement (i.e., duties, specialized experience statements, job analyses, assessment questions, and selective placement factors) for ONCP to recruit for positions within ONCP Divisions.
d. Assists and provides solutions to the ONCP hiring managers on all recruitment processes.
e. Provides HR recommendations and resolves personnel actions within ONCP, as well as resolves complex or simple informal complaints.
f. Explains human resources policies, procedures, laws, and standards to new and existing employees.
g. Process all personnel action forms and ensuring proper approval.
h. Oversees hiring process, which includes coordinating job posts, reviewing resumes, and performing reference checks.
i. Provides Excellent Customer Service.
j. Coordinates with OCHCO on all HR matters.
k. Collect and organize information about ONCP-BMD problems to be solved or the procedure to be improved
l. Analyze data gathered and develop solutions or alternative methods of proceeding
m. Recommend new systems, procedures, or organizational changes

4. TASKS:

It is anticipated that most of the work to be performed under this Task Order will align with the organizational structure of BMD, as follows. Support for the various Task Areas may cross Branches and the Executive Office of the BMD Division Director, as necessary, to support the BMD program.

a. Portfolio Management Oversight for Acquisitions Management Branch (ACMB)
b. Project Management (clearly defined budget at outset, completed in a specific timeframe) Support Acquisitions Management Branch (ACMB)
c. Program Management (typically does not have an end date, delivered benefits are on-going) Support for the ACMB
d. All programs align with ONCP strategic goals
e. Communication Support in support of all branches but directly tasked from BMD Division Director
f. Financial and Budget Management Support in support of the Financial Management Branch (FMB)
g. Acquisition Management Support for Acquisitions Management Branch (ACMB)

h. Asset and Property Management Support for Asset Management Branch (AMB)

i. Human Resources Management Support for Human Resource Management Branch (HRMB)

5. TASK AND DELIVERABLE SCHEDULE:

Description	Approval Required	Draft Due Date	Final Due Date	Copy To/Participants
Kick-Off Meeting	No	N/A	10 business days after award	COR/CO
Project Management Plan	Yes	Kick Off Mtg	5 business days after Kick-Off Meeting, and updated with contract life cycle	COR
Monthly Status Reports	No	N/A	15 days of each month	COR/CO
Monthly Status Report Meetings	No	N/A	20th day of each month	COR/CO
Task Closeout Report	Yes	15th day after contract closeout	5 days after receipt of Government comments on Draft Closeout Report	COR/CO
Situation Reports	Yes	TBD (as tasked)	TBD (as tasked)	COR
Other Deliverables to be Specified in Written Technical Direction	Yes	TBD (as tasked)	TBD (as tasked)	COR

6. FEDERAL HOLIDAYS

Unless specifically authorized in writing by the Contracting Officer, no services will be provided and no charges will be incurred and/or billed to any order on this contract on any of the Federal Holidays listed below.

New Year's Day	**Labor Day**
Martin Luther King Day	**Columbus Day**
Presidents' Day	**Veterans' Day**
Memorial Day	**Thanksgiving Day**
Juneteenth	**Christmas Day**
Independence Day	

7. PERIOD OF PERFORMANCE

The period of performance for this contract will be one base year from date of award with optional three years, 07/01/2023 – 06/30/2027.

8. PLACES OF PERFORMANCE:

Primary:

The Primary Place of Performance for all Labor Categories will be FEMA HQ, Washington, D.C.

Secondary as needed and approved by COR:

Other work may occasionally be performed at Mt. Weather, and other Federal, State, and territorial work sites and contractor facilities.

9. TRAVEL

The Government will not reimburse the Contractor for travel to/from or parking at the primary place of performance. Local travel costs or parking for temporary duty assignments within the local commuting area will not be reimbursed under this contract. For this contract, the local commuting area is defined as a temporary duty station outside of the "primary place of performance", but within the vicinity surrounding it. If the site is a driving distance of less than 50 miles, by the most direct route, from the primary place of performance, the site is a part of the local commuting area. Contractor travel beyond the local commuting area shall be required to support this Contract. 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 (FTR). The Contractor shall be responsible for obtaining COR approval (electronic mail is required) in advance of each travel event. Travel between U.S. States, U.S. Territories and Outside the Continental U.S. (OCONUS) may be required. The Contractor shall provide documentation for travel expenses, including receipts, to support travel reimbursement upon request.

Use of Government Vehicles. In the performance of this requirement, the contractor may be required to operate FEMA vehicles such as passenger vehicles, vans, sports utility vehicles, box trucks, and an open gate truck. If tasked to operate government-owned vehicles, the contractor will be held liable for any costs associated with misuse of Agency vehicles and must provide proof of liability insurance coverage. Additionally, the contractor must obtain prior approval from the COR to use Agency vehicles, and must restrict their use to official purposes, only in performance of the Task Order.

10. GOVERNMENT FURNISHED EQUIPMENT

For work performed at Government facilities, FEMA will provide laptop computers,

communications equipment, workstations, and applications needed for e-mail and day-to-day work. All equipment will be identified, and the Contractor will need to track GFE in accordance with FEMA Property Management Directive -119-7.

11. CLEARANCES AND OTHER TERMS AND CONDITIONS

This clause applies to the extent that this contract involves both unclassified and classified information. Personnel supporting this contract, will require access to information not to exceed the security access level of **TOP SECRET, or SENSITIVE COMPARTMENTED INFORMATION**.

This SOW requires clearance at the TOP SECRET level. A Top-Secret Facility Clearance is required of the Prime Contractor, and for any subcontractors to provide cleared contractor personnel to work under this Task Order. Due to the applications and systems that will be developed and tested, all of the contractor staff must hold clearances at the TOP SECRET level, and **some, but not all**, must have the capability of obtaining Secret Compartmented Information (SCI). **Specific positions requiring Top Secret/SCI clearances will be specified through written Technical Direction.**

Contractor employees working on-site or visiting Government facilities shall wear an identification badge that, at minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times. Contractor personnel shall identify themselves as Contractors in any telephone or e-mail communications when using Government equipment or systems.

12. PRIVACY

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 and 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.

Clauses
1) Safeguarding of Sensitive Information (MAR 2015)
2) Information Technology Security and Privacy Training (MAR 2015)
3) FAR 52.204-9 Personal Identity Verification Of Contractor Personnel (JAN 2011)
4) FAR 52.224-1 Privacy Act Notification (APR 1984)
5) FAR 52.224-2 Privacy Act (APR 1984)
6) FAR 52.224-3 Privacy Training
7) HSAR 48 CFR 3052.204-71 Contractor Employee Access

Safeguarding of Sensitive Information (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) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" 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 PII 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.

PII is a subset of sensitive information. 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);

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);

(2) 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

(3) 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 http://www.dhs.gov/dhs-security-and-training-requirements-contractors, 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 *Version 13.2, September 20, 2022*

(3) DHS Security Authorization Process Guide

(4) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(5) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(6) DHS Information Security Performance Plan (current fiscal year)

(7) DHS Privacy Incident Handling Guidance

(8) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(9) 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

(10) 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. 4300B.200 Communication Security (COMSEC) version 5.0 National Security Cyber Division (dhs.gov)

(11) 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* version 13.2 2022 and attachments 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.

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

(13) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security 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.

(14) 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.

(d) *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 CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current 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 13.2, September 20, 2022*, 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 Requirements Traceability Matrix and Government security documentation templates. 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.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in 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. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, 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.

(3) *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.

(4) *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.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this

contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal 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 Federal reporting requirements for Contractor systems.

(e) *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; and

(xiv) Any additional information relevant to the incident.

(f) *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.

(g) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability 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.

(2) 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:

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) 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

(vi) Information identifying who individuals may contact for additional information.

(i) *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 was under the control of the Contractor or 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:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) 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.

(j) *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*.

(k) "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.

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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.

Security Training Requirements.

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.

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 capable 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.

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.

(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 nationalor 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 oran 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 SecurityAct, 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 andControl 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 orhis/her designee);

(3) Information designated as "For Official Use Only," which is unclassified informationof a sensitive nature and the unauthorized disclosure of which could adversely impacta 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, computerdrives, network software, computer software, software programs, intranet sites, and internetsites.

(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 todetermine 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 ITresources 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 onthe 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 duringand after Task Order performance.

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

Alternate I

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this Task Order or approved by the COR in writing as necessary for performance of the work under this Task Order. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statementof work, other terms and conditions in this Task Order, or as approved in writing by the COR,is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the Task Order and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right,a guarantee of access, a condition of the Task Order, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold andsave DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the Task Order, unless a waiverhas been granted by the Head of the Component or designee, with the concurrence of both theDepartment's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U. S.citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after Taskorder award shall be reported to the Contracting Officer.

(End of clause)

52.204-9 Personal Identity Verification of Contractor Personnel.

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

(1) When no longer needed for contract performance.

(2) Upon completion of the Contractor employee's employment.

(3) Upon contract completion or termination.

(c) The Contracting Officer may delay final payment under a contract if the Contractor fails to comply with these requirements.

(d) The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. It shall be the responsibility of the prime Contractor to return such identification to the issuing agency in accordance with the terms set forth in paragraph (b) of this section, unless otherwise approved in writing by the Contracting Officer.

(End of clause)

52.224-1 Privacy Act Notification.

As prescribed in 24.104 , insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of1974, Public Law93-

579, December 31,1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)

52.224-2 Privacy Act.

As prescribed in 24.104 , insert the following clause in solicitations and contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function:

PRIVACY ACT (APR 1984)

(a) The Contractor agrees to-

(1) Comply with the Privacy Act of1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency

(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that

contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing Privacy at DHS: Protecting Personal Information accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or

otherwise

handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

13. SECURITY LANGUAGE

All personnel require access to information at the TS level. Contractor must ensure contractor employees' personnel clearances are commensurate with required clearance 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.

DD254 Information:

Contractor access to classified information is required under this task order. Several on site Government locations in which work under the task order is to be performed include areas authorized for TS materials and information. Therefore, Contractor personnel, working under this order which specify the need for a Top Secret or SCI security clearance, must possess a final U.S. Government Top Secret clearance based on a current Single Scope Background Investigation.

As an employee of the Federal Government or one of its contractors, licensees, or grantees who occupies a position which requires access to classified information, each employee will be the subject of a personnel security investigation. The purpose of this investigation will determine your trustworthiness for access to classified information. When the investigation is completed, Defense Security Services will grant you a security clearance based upon a favorable determination of the investigation results. By being granted a security clearance, an employee will have met the first of three requirements necessary to have access to classified information.

The second requirement each employee must fulfill is to sign a "Classified Information Nondisclosure Agreement," the SF 312. "All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access." This requirement is reiterated in the executive order on classified national security information. The SF 312 is a contractual agreement between the U.S. Government and the cleared employee, in which the employee agrees to never disclose classified information to an unauthorized person. For employees requiring access to TS/SCI; the employee will be required to sign a separate NDA for Standard Form 4414.

The third and final requirement for access to classified information is the "need-to-know;" that is, employees must have a need to know for classified information in order to perform their official duties.

Deliverables produced under this work order shall be classified in accordance with security classification instructions and procedures provided by FEMA OCSO Security Compliance Division. A current DD Form 254, Contract Security Classification Specification, must be issued and placed on file with FEMA's Industrial Security Officer prior to award of the order.

The Contractor shall meet and comply with all applicable physical, personnel, industrial, and other security requirements outlined in:

a. DD 254, Contract Security Classification Specification

b. DHS MD 4300A Sensitive Systems Handbook, Version 5.5, September 30, 2007

c. Federal Information Security Management Act of 2002 (FISMA)

d. NIST Special Publication 800-37 May 2004

e. Homeland Security Presidential Directive/Hspd-7 Critical Infrastructure Identification, Prioritization, and Protection, Dec 17, 2003.

f. FAR 52.204-2 Security Requirements

g. Standard Form 312, Non-Disclosure Agreement

h. Standard Form 4414, TS/SCI Non-Disclosure Agreement

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:
Unauthorized Disclosure of Classified Information and Controlled Unclassified Information (usalearning.gov)

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 OPSEC Awareness for Military Members, DOD Employees and Contractors (usalearning.gov)

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: Insider Threat Awareness (usalearning.gov)

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:

a. the investigation was completed within the last five years,
b. it meets or exceeds the minimum requirement for the position they will occupy or functions they will perform on this contract,
c. the contractor personnel have not had a break in employment since the prior favorable adjudication, and,
d. 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:

a. Standard Form 85P, "Questionnaire for Public Trust Positions"
b. Optional Form 306, "Declaration for Federal Employment"
c. SF 87, "Fingerprint Card" (2 copies)
d. DHS Form 11000-6, "Non-Disclosure Agreement"
e. 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 contactor 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.

14. 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 has determined to be a potential security threat.

15. 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) must return such identification to FEMA as soon as any of the following occurs:

a. When no longer needed for contract performance.

b. Upon completion of a contractor employee's employment.
c. 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.

16. DD254 INFORMATION

Contractor access to classified information is required under this contract. Several on site Government locations in which work under the contract is to be performed include areas authorized for TOP SECRET materials and restricted to protect LIMITED DISTRIBUTION information. Therefore, all Contractor personnel, working tasks under this contract must possess a final U.S. Government TOP SECRET clearance based on a current Single Scope Background Investigation.

ADDITIONAL SECURITY REQUIREMENTS. DHS/FEMA PSO CONCURS AND APPROVES THE SPECIAL ACCESS PROGRAM SECURIY REQUIREMENTS FOR THIS CONTRACT. Clearances: Access to SAP information requires a final US Government c1earance at the appropriate classification level. Subcontracting: The DHS/FEMA PSO must approve Subcontracting requests prior to award AND the DHS/FEMA PSO must review and approve all SAP Subcontracting DD-254s prior to pass-down from the Prime contractor. No storage, processing, or access to SAP information is authorized at the contractor location. All information, products, and deliverables will remain the sole property of the Government. Deliverables produced under this contract shall be classified in accordance with security classification instructions and procedures provided by the COR. A current DD Form 254, Contract Security Classification Specification, must be on file with FEMA's Industrial Security Officer prior to award of the contract. The Contractor shall meet and comply with all applicable physical, personnel, industrial, and other security requirements outlined in:

a. DD 254, Contract Security Classification Specification
b. DHS Sensitive Policy Directive 4300A September 2022
c. DHS 4300A Sensitive Systems Handbook, Version 12.0, November 15, 2015
d. Federal Information Security Management Act of 2014 (FISMA)
e. NIST Special Publication 800-37 Rev 1 February 2010
f. Homeland Security Presidential Directive/HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection, Dec 17, 2003.
g. FAR 52.204-2 Security Requirements DHS has exclusive security responsibility for all SAP classified material released to or developed under this contract. DHS is relieved of security inspection responsibility for all such material. DHS retains oversight/inspection

responsibilities for facility clearance requirements and collateral information outside of DHS facilities.

DHS/FEMA/CONCURS AND APPROVES THE "NEED-TO-KNOW" AT THE SCI LEVEL"" Clearances: Access lo Intelligence information requires a final US Government clearance. Subcontracting: Subcontracting requires prior approval of the GCA. Briefings: Special briefings and procedures are required. No storage or processing of SCI is authorized at contractor location.

Documents generated that are related to this project shall include, as a minimum, the protective footer marking, "(FOUO) For Official Use Only," unless otherwise directed by the Government.

16a. DD FORM 254 ACCESS REQUIREMENTS

The Contractor will require access to:	**YES**	**NO**
COMMUNICATIONS SECURITY INFORMATION {COMSEC)		X
RESTRICTED DATA		X
CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
FORMERLY RESTRICTED DATA		X
INTELLIGENCE INFORMATION-SENSITIVE COMPARTMENTED INFORMATION (SCI)		X
INTELLIGENCE INFORMATION - NON (SCI)	X	
SPECIAL ACCESS INFORMATION		X
NATO INFORMATION		X
FOREIGN GOVERNMENT INFORMATION		X
LIMITED DISSEMINATION INFORMATION	X	
FOR OFFICIAL USE ONLY INFORMATION (FOUO)	X	
In performing this contract, the contractor will:	**YES**	**NO**
RECEIVE CLASSIFIED DOCUMENTS ONLY		X
RECEIVE AND GENERATE CLASSIFIED DOCUMENTS		X
FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
PERFORM SERVICES ONLY		X
HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S.		X
POSESSIONS AND TRUST TERRITORIES		
BE AUTHORIZED TO USE THE SERVICES OF THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC)		X
OR OTHER SECONDARY DISTRIBUTION CENTER		
REQUIRE A COMSEC ACCOUNT		X

HAVE TEMPEST REQUIREMENTS		X
HAVE OPERATIONS SECURITY REQUIREMENTS (OPSEC)	X	
BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
HAVE ACCESS TO CLASSIFIED INFORMAION ONLY AT A GOVERNM ENT ACTIVITY	X	

17. ADDITIONAL SECURITY STANDARDS REFERENCES:

1. In general, work shall be compliant with DHS and FEMA security policies, requirements, authorities, references, and guidance listed below:

   a. DD 254, Contract Security Classification Specification;

   b. DHS Sensitive Policy Directive 4300A Version 13.1 July 27, 2017;

   c. DHS 4300A Sensitive Systems Handbook, Version 12.0, November 15, 2015;

   d. Federal Information Security Management Act of 2002 (FISMA);

   e. NIST Special Publication 800-37 Rev 1 February 2010;

   f. Homeland Security Presidential Directive/HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection, Dec 17, 2003; and,

   g. FAR 52.204-2 Security Requirements.

   h. Presidential Policy Directive - 40 (PPD-40), National Continuity Policy, July 15, 2016;

   i. Homeland Security Council - National Continuity Policy Implementation Plan - August 2007;

   j. Federal Continuity Directive 1 (FCD 1)- Federal Executive Branch National Continuity Program and Requirements - January 17, 2017;

   k. Federal Continuity Directive 2 (FCD 2) - Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process - June 13, 2017;

   l. GAO Report, Performance Measurement and Evaluation, May 2005;

   m. Section 3541 of title 44, United States Code, "Federal Information Security Management Act of 2002" (FISMA);

   n. Department of Defense Directive 8100.1, Global Information Grid (GIG) Overarching Policy, "September 19, 2002;

o. Department of Defense Directive 8500.1, "Information Assurance (IA), "October 24, 2002;

p. Continuity Guidance Circular 1 (CGC 1) - Continuity Guidance for Non-Federal Governments -February 2018;

q. Continuity Guidance Circular 2 (CGC 2)- Continuity Guidance for Non-Federal Entities: Mission Essential Functions Identification Process - October 2013;

r. Project Management Body of Knowledge (PMBOK) - Project Management Institute (PMI).

18. 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. The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all 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. 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

multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

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.

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 1194.2(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 approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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.

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.

11. 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 agreement.

19. SECTION 508 REQUIREMENT

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, 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 standards have been identified:

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 1194.24 - Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or

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.

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.

20. DHS ENTERPRISE ARCHITECTURE COMPLIANCE REQUIREMENTS

a. "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.

b. Description information for all data assets, information exchanges and data standards, whether
adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

c. 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.

e. 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."