Federal Emergency Management Agency (FEMA)
Mission Support Enterprise Data Analytics & Strategic Communications Support Services
Performance Work Statement (PWS) (TO# for BPA#70FA6022A00000002)

1. PURPOSE

The purpose of this procurement is to secure strategic communications support services for the Office of the Chief Information Officer (OCIO). The OCIO includes five Portfolios: IT Management, Office of the Chief Information Security Officer (OCISO), Operations, and Office of the Chief Technology Officer (OCTO).

The services performed under this task order will enable the Mission Support Enterprise to develop and deliver high quality strategic communications, reports, and briefings.

2. BACKGROUND

The Office of the Chief Information Officer (OCIO) provides enterprise IT services vital to carrying out FEMA's mission for both disaster survivors and FEMA employees. This includes providing secure IT capabilities so that FEMA IT is "always ready" to support our stakeholders and workforce.

This Performance Work Statement (PWS) outlines the Federal Emergency Management Agency (FEMA) Office of Chief Information Officer (OCIO)'s requirements for Strategic Communications. Strategic communications activities are integral to the successful operation of the organization and each Component must continue to build its competency in these areas to maximize its ability to support both internal and external stakeholders.

3. APPLICABLE DOCUMENTS

All applicable documents required to complete the tasks below will be provided to the contractor following award.

4. SCOPE

The Contractor shall provide expert services to the OCIO Components including general program/project management, data analysis and reporting, strategic communications development, and data visualization support activities.

5. PERFORMANCE REQUIREMENTS SUMMARY (PRS)

This contract includes a Performance Requirements Summary (PRS) at PWS 10. The PRS plays an integral role in the administration of the contract. In addition to any applicable inspection clauses or other related terms and conditions contained in the contract, the PRS shall serve as a primary tool for inspection and acceptance of services as facilitated by the Contracting Officer's Representative (COR). Evaluation of the Contractor's overall performance shall be in accordance with the performance standards set forth in the PRS, and will be conducted by the COR. The

PRS constitutes a material aspect of the contract and will not be changed or otherwise modified without prior written approval from the Contracting Officer.

6. SPECIFIC TASKS

Task 1: Strategic Communications (CLIN0001)
Assist OCIO with establishing a formalized strategic communications capability for Components to effectively communicate messages internally and externally and build the organization's brand at FEMA. These activities include the assistance with, but are not limited to the following:

- Collaborating with leadership and key stakeholders to identify and define strategic communications vision and approach (i.e., around priority initiatives, process change or adoption, general increased transparency, and information sharing, etc.)
- Supporting development of formal strategic communications plan, corresponding templates, change management products, and communications to support desired engagement based on identified needs and initiatives
- Enhancing and/or tailoring existing materials, and support development and review of executive briefings, presentations, communications, letters, reports, and other products as required
- Proofing for clarity, proper grammar, polished nature of final documents, consistency with prior documents, and consistency with OCIO professional standards
- Communicating key messages to leadership and stakeholders based on data analytic insights
- Providing any additional research/support to inform development of communications
- Supporting processes and schedule to efficiently draft, review, approve, and deliver communications
- Supporting ad hoc priority communications development (i.e., papers, web content, executive briefings, presentations, communications, letters, reports and memos to FEMA leadership, Congress, etc.)

7. OPTIONAL REQUIREMENT – SURGE

The Contractor upon request from the Contracting Officer (CO) and COR shall provide additional personnel to meet adhoc and surge requirements. Within the scope of this requirement, adhoc and surge requirements will most certainly arise during the life of this contract. These situations will require the Contractor to respond with very little notice.

8. PERIOD OF PERFORMANCE

The period of performance for this requirement shall have a one (1) year base period with one (1) one (1) year option periods.

9. CONTRACT TYPE

The contract type for this Task Order will be Firm-Fixed Price (FFP).

10. GOVERNMENTFURNISHED EQUIPMENT AND INFORMATION

The Government will provide accommodations as necessary at FEMA HQ, 500 C. St. SW Washington D.C. 20472 and satellite locations for critical working sessions, key meetings and presentations as deemed appropriate by FEMA authorized personnel.

Desks, chairs, local telephone service, and necessary computer and office equipment will be provided for assigned personnel. Contractor computer or its assets are not authorized for use on this effort without the pre-approval of the COR and screening by DHS/FEMA/cyber security.

11. PERFORMANCE REQUIREMENTS SUMMARY

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

Service Output	Performance Objective	Acceptable Quality Level (AQL)	Positive Incentive	Negative Incentive
1. Strategic Communications	Assist OCIO with establishing a formalized strategic communications capability for Components to effectively communicate messages internally and externally and build the organization's brand at FEMA.	98%	Positive CPARS assessment	Negative CPARS assessment

12. PLACE OF PERFORMANCE

The work will be performed at contractor offices and/or FEMA headquarters.

Note: The Contractor is authorized to telework at the discretion of the Government.

13. KICKOFF MEETING

The Contractor shall attend a Kickoff Meeting with the Contracting Officer, Contracting Officer's Representative, and/or other designated representatives within five (5) business days of notification of award. The Kickoff Meeting will be held at the Government's facility or virtually as determined by the Government. Attendance by the designated "key" contractor personnel is required at the Kickoff Meeting.

14. REPORTING REQUIREMENTS/DELIVERABLES

Deliverable	Delivery Schedule	Approved By
Project Management Plan	**Draft** – with the Technical Proposal **Final** – two weeks after the Start-Of-Work	COR
Technical Progress Report	Bi-weekly, on or before the 1st and 15th calendar day of each month	COR
Ad Hoc Reports	Upon request	COR
Final Project Close-out Report	Five business days prior to end of Task Order	COR

Description:

Project Management Plan (PMP): The Contractor shall develop and maintain the PMP and/or OCIO Project schedule. A draft PMP shall be submitted with technical proposal and final PMP shall be submitted two (2) weeks after the Start-of-Work meeting. Revisions may be required at the request of FEMA COR. The Contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given.

The PMP shall include the management approach, organizational resources, and management controls to be employed to meet the performance (to include quality and risk elements) and schedule requirements for this effort. The PMP shall detail the deliverables, methods for developing deliverables, allocation of staff and other resources necessary to produce the deliverables and a revised timeline for producing the deliverables, if deemed necessary. The COR and federal PM shall receive the revised PMP in electronic form.

The Contractor shall update the PMP and/or OCIO Project schedule, as requested by FEMA. The Contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given.

Technical Progress Report: The Contractor shall provide bi-monthly Technical Progress Reports to the Program Manager (PM) and Contracting Officer's Representative (COR) on or before the 1st and 15th calendar day of each month via hard copy and electronically (Excel,

Word, Access, Power Point) as applicable. The Technical Progress Report shall include the following:

- A concise statement identifying work performed and work products delivered and accepted during the reporting period.
- An outline of work to be accomplished during the next reporting period.
- A description of any problem encountered or anticipated that will affect the completion of any individual task within the time and fiscal constraints as set forth in the work order, together with recommended solutions or a statement that no problems were encountered.

Ad Hoc Reports: The Contractor shall provide the COR with a status report as requested for any tasking within the scope of this Contract upon request. Furthermore, if the Contractor is unable to adhere to said stipulation the Contractor shall submit written justification to include specific time of delivery.

Final Project Close-out Report: This report will encompass all phases and tasks completed with a summation of accomplishments.

15. TRAVEL

The Contractor will not be required to travel outside of the National Capital Region (NCR) under this task order.

16. GOVERNMENT POINTS OF CONTACT (Do not contact directly during solicitation stages)

Points of Contact (POC):

Primary POC:

[redacted]

Alternate POC:

[redacted]

Contractor Officer's Representative (COR):

[redacted]

Contracting Officer (CO):

[redacted]

17. ACCEPTANCE CRITERIA

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

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

The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver.

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

18. PERSONNEL REQUIREMENTS

The Contractor shall provide staff with senior-level experience and ability, preferably in federal government organizations, in the following areas of specialty and skills:

- Advanced proficiency with Microsoft Office Suite
- Advanced design and/or development, as applicable, in Visio, as well as SharePoint, InfoPath, and other web-based tools with a preference for the ability, certifications, and credentials to be granted access to develop web applications on the FEMA intranet site
- Strategic communications with internal stakeholders (e.g., business partners, employees) and external oversight bodies (e.g., Congress, auditing agencies)
- Advanced writing and editing

The Contractor must have the ability to work in a dynamic, fast-paced, and challenging environment. The Contractor personnel shall interface with agency senior officials, internal staff, and employees, and other supportive contracted staff, at all levels. Therefore, the Contractor personnel must be flexible and adaptable to changes and have customer service expertise.

During the first ninety (90) calendar days, the Contractor shall not make any personnel changes unless an individual's sudden illness, death, or termination of employment necessitates such substitutions. In such cases of these occurrences, the Contractor shall notify the Program Manager and COR promptly and submit documentation pertaining to the proposed substitution in writing at least fifteen (15) calendar days in advance, and thirty (30) calendar days in advance if security clearances are to be obtained in advance of the proposed substitution.

The Contractor must provide a detailed explanation of the circumstances causing the proposed substitution, along with resumes. All resumes submitted for each proposed substitution must have qualifications that are equal to or superior to the qualifications of the person for whom the substitution is being made. The Program Manager shall evaluate the resume of each request to verify the qualifications of every new employee being assigned to this task order.

Personnel Security: Security requirements shall be based on current DHS and FEMA policy for contractors.

Employee Citizenship: Each employee of the contractor working on the contract shall either be a citizen of the United States of America or currently be a lawful resident.

19. KEY PERSONNEL

Communications Lead:
The Contractor shall propose a Communications Lead to facilitate Government-Contractor communications. The Communications Lead will be the primary technical and managerial interface between the Contractor and Contracting Officer (CO) and the Contracting Officer's Representative (COR). This person, and an alternate or alternates who shall act for the Contractor when the Communications Lead is absent, must have full authority to act for the Contractor on all Contract matters relating to daily operations.

Specialized experience includes expertise in the management and control of funds and resources using complex reporting mechanisms, demonstrated capability in managing multi-task contracts and/or subcontracts of various types and complexity. Assigned Communications Lead must demonstrate the ability to work independently or under only general direction. Resume must show thorough experience in performing the following:

- Managing clients
  - Building a knowledge base of each client's business, organization, and objectives
  - Managing day-to-day client interaction
  - Setting and managing client expectations
  - Communicating effectively with clients to identify needs and evaluate alternative business solutions
  - Continually seeking opportunities to increase customer satisfaction and deepen client relationships
- Achieving operational objectives and contributing information and recommendations to strategic plans and reviews
- Implementing productivity and quality standards

- Providing technical direction and guidance to contractor staff to ensure Contract requirements and expectations are clear, success criteria are defined, progress toward results are monitored, and that all activities are performed in compliance with the terms of the Contract
- Identifying risks and appropriate mitigation strategies
- Meeting financial objectives by forecasting requirements, preparing budgets, scheduling expenditures, analyzing variances, and initiating corrective actions
- Managing a multi-tiered project and/or multiple projects simultaneously

Required Education: Minimum of 7 years of relevant experience and bachelor's degree in Computer Science, Information Systems, Engineering, Business, Education, Management Sciences, Psychology, Human Resources Development/ Management, or other related discipline or equivalent experience in a technical or business discipline.

20. ADDITIONAL PERSONNEL REQUIREMENTS

Qualified Personnel and Labor Categories - It is the responsibility of the Contractor to propose qualified Contractor personnel to perform all requirements specified in the PWS. Qualified personnel should have significant experience in the support services related to this scope and must be approved by the Government.

21. GENERAL REQUIREMENTS

All content, instruments, processes, studies or other tools and deliverables developed under this contract (to include, without limitation, any survey questionnaires, sampling methodologies, participant lists and resulting analysis) shall be the sole property of the Federal Emergency Management Agency. As such, these materials may be used by FEMA and, upon FEMA direction, its contractors, for future research studies, product development and program initiatives.

The Contractor shall provide quality control proofreading and editing for all products in accordance with Associated Press (AP) Style rules. In addition, it is expected that for printed products, the contractor shall provide the project officer with Government Printing Office (GPO) Form 952 (Desktop Publishing Disk Information) and the final print ready product in specified format (e.g., electronic files, camera ready art negatives, CD-ROM master) along with graphics and printing specifications. All projects shall be sourced through the GPO. The contractor shall meet the requirements of Title 44, Government Printing and Binding Regulations, and coordinate with and obtain approval from the Agency Printing officer and the Project officer for all printing.

All materials, including new photography, videography and imagery, and graphic elements, created under this contract are the property of the Federal Emergency Management Agency and may be modified, reproduced, and disseminated without restriction.

22. CONFIDENTIALITY

All information regarding this effort must be regarded as sensitive information by the Contractor and must not to be disclosed to anyone outside the Contractor's organization without the written permission of the Contracting Officer.

Contractor personnel assigned to this effort will be required to sign a "Non-Disclosure Agreement".

23. QUALITY ASSURANCE

The Contractor shall ensure overall quality of work performed. All support and related activities performed under this Contract will be planned, controlled, and documented as required by existing regulations and guidelines.

24. END OF PERFORMANCE

All information, as well as Contractor working papers, shall be returned at the end of the Contract. Any Contractor storage drives used in the performance of this contract shall be provided to FEMA for removal of FEMA information.

25. SECTION 508 AND 504 COMPLIANCE

Accessibility Requirements (Section 508)
Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.
All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards
36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.
36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of

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

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

Section 508 Compliance Requirements
36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

Section 504 Compliance Requirements
The Contractor/Provider shall comply fully with Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities. No otherwise qualified individual with a disability shall, solely by reason of his or her disability, be excluded from participation in, be denied the benefits of, or subjected to discrimination under any program or activity for which the Contractor/Provider is awarded a contract and/or receives federal financial assistance from the Federal Emergency Management Agency. This includes, but is not limited to, providing reasonable

accommodations and modifications to ensure effective communication access, physical access, and program access to all participants, including persons with disabilities. The Contractor/Provider shall incorporate this language in any subcontracts related to the provision of the FEMA public-facing program or activity.

26. PRIVACY

The collection and use of information described in this contract does not concern the collection, maintenance, dissemination, or use of PII other than as described in this contract for access to Outlook. Prior to any other access, collection, maintenance, dissemination, or use of PII (as defined in DHS policy) pursuant to this contract, the contractor will enter into an Information Sharing and Access Agreement (ISAA) approved by the FEMA Privacy Office and the contractor and COR, in consultation with the FEMA Privacy Office, will obtain an adjudicated PTA (as well as PIA and SORN coverage where applicable)."

To accomplish the tasks outlined in this contract, FEMA will provide the contractor access to the names of the appropriate Government staff. This information sharing is authorized by The Homeland Security Act of 2002, 6 U.S.C. 313, 314, 317, 320, 321a, and 711; Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. 5144, 5149, 5170b, 5192, and 5197; and Routine Use F of the DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792March 16, 2018, 83 FR 11780 PIA DHS/ALL-015 Web Portal, PIA DHS/ALL-059 Employee Collaboration Tool, Routine Use F of the DHS/ALL 016 Correspondence Records September 26, 2018 83 FR 48645.

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.

27. UNCLASSIFIED INFORMATION ACCESS / FOUO ACCESS

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

Unauthorized Disclosure of Classified or Unclassified Information:
Contractors and Subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training.
Access to the training can be obtained at:
https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm
Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

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

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

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

The contractor will:

1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.
2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

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 11000-25, "Contract Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 11000-25 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

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

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

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

For those contractor personnel who do not have an acceptable, prior, favorable adjudication or who otherwise require reinvestigation, FEMA PSD will issue an electronic notification via email directly to the contractor applicant/personnel that contains the following documents, which are incorporated into this contract by reference, along with a link to the National Background Investigation Services (NBIS) e-Application (eAPP) online system and instructions for submitting the necessary information:

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

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the National Background Investigation Services (NBIS) e-Application (eAPP) online 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.

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.

Separation of 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:

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

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

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

Unauthorized Disclosure of Classified or Unclassified Information
Contractors and Subcontractors who are working on this contract shall receive the Unauthorized Disclosure of Classified or Unclassified Information training.
Access to the training can be obtained at:
https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm
Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

28. Security Training

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

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 (COR), before the contractor or subcontractor is granted access to classified or unclassified information but no later than 30 calendar days after awarded contract. Send certificates of completion for Unauthorized Disclosure, OPSEC, and Insider Threat to the FEMA COR no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

Unauthorized Disclosure of Classified or Unclassified Information
Contractors and subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training.
Access to the training can be obtained at:

https://securityawareness.usalearning.gov/disclosure/index.html

OPSEC Training
Contractors and subcontractors who are working on this contract shall receive the OPSEC Awareness Brief.
Access to the briefing can be obtained at https://securityawareness.usalearning.gov/opsec/
Insider Threat Training
Insider Threat training for contractors can be found at:
https://securityawareness.usalearning.gov/itawareness/index.htm#

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 shall:

1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.
2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

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.

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

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

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later

than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources 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.

HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information (July 2023)

(a) Definitions. As used in this clause—Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability

Information (CVI) as defined in 6 CFR part 27, ''Chemical Facility Anti-Terrorism Standards,'' and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual ''Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information'' dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Public Law 116– 283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, ''Protection of Sensitive Security Information,'' 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 designee), including Department of Homeland Security MD 11056.1, ''Sensitive Security Information (SSI)'' and, within the Transportation Security Administration, TSA MD 2810.1, ''SSI Program'';

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;
(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

> (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems

and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or
(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.
(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual. Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form. Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency. Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.
Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.
Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) Handling of Controlled Unclassified Information. (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhssecurity-

and-training-requirements contractors

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

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

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) Incident Reporting Requirements.

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-trainingrequirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a FIPS 140–2/140–3 Security Requirements for Cryptographic Modules validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems, 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) Unique Entity Identifier (UEI);
(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, and email);
(v) Contracting Officer POC (address, telephone, and 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 CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.
(d) Incident Response Requirements.

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting 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 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;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data

shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

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

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information. Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, Guidelines for Media Sanitization, Appendix G.

(f) Other Reporting Requirements. Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) Subcontracts. The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(h) Authority to Operate. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023), or any successor publication; and the Security Authorization Process Guide, including templates. These

policies and templates are accessible at https://www.dhs.gov/dhs-security-and-trainingrequirements- contractors.

(i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package 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). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the information 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 SP 800–53, Security and Privacy Controls for Information Systems and Organizations, or successor publication, accessible at https://csrc.nist.gov/publications/sp. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters- CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or
(ii) Submitting the updated SA package directly to the COR.

(3) Security Review. The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity

by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images),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) Federal Reporting and Continuous Monitoring Requirements. Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhssecurity-and-training-requirements contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

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:

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

C. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR

Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

4. FEMA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of FEMA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to FEMA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the SOW. 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 SOW. 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.

c

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

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

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

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