Statement of Work
CCS Program (CCSP)
Task Order One
Federal Emergency Management Agency
Office of the Chief Administrative Officer

Department of Homeland Security
Office of Health Security
Total Workforce Protection Directorate

1. BACKGROUND

Under the congressionally enacted Public Law 107-67, Sec. 630, on November 12, 2001, Federal agencies are permitted to administer a program to assist their lower income Federal employees with the cost of childcare. The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) employs approximately 10,000 employees. Most of these employees work in the Continental United States, but there are DHS FEMA employees in Alaska, Hawaii, Puerto Rico, the United States Virgin Islands, Guam, and other overseas locations. A CCS Program (CCSP) will ensure the FEMA workforce has dependable and affordable childcare is critical their successful execution of FEMA's various missions by promoting their presence and be mission ready.

2. SCOPE

The scope of this effort is to establish the CCSP program for all eligible DHS FEMA employees, which also includes the administration of the program, marketing, and obtaining and maintaining the Authorization to Operate (ATO). The resultant FEMA Task Order One under DHS FEMA Category Management & Strategic Sourcing department wide acquisition vehicle and CCSP Solicitation 70RWMD24QP0000007 Blanket Purchase Agreement (BPA) has the potential to support up to 5,300 program participants and will have a staggered roll-out to provide the CCSP across all DHS components.

This SOW does not constitute a personal services contract. As such, in accordance with Federal Acquisition Regulation (FAR) 37.104, the Schedule Contractor awarded this CCSP Solicitation 70RWMD24QP0000007 Blanket Purchase Agreement (BPA) shall exercise relatively continuous supervision and control over its Schedule Contractor personnel. Contractor personnel are not Government employees. The Schedule Contractor shall provide all services, personnel, supplies and necessary equipment (except as set forth herein) to complete the duties as described by the SOW CLINS below:

CLIN 0001	Childcare Subsidy Program Payments NTE 29 Participants (Section 3)
CLIN 0002	Service Charge Basic Fee NTE 199 Participants (Section 4)
CLIN 0003	Childcare Subsidy Program Payments NTE 170 Participants (Section 3)
IMPORTANT NOTE:	CLIN 0003 Subject to the Availability of Funds

3. SPECIFIC TASKS

The Schedule Contractor shall provide childcare managed services with existing cloud-based platform providing the minimum capabilities outline below:

1. *Secure record retention of completed materials*
2. *Receive and process new applications and recertification documents within ten (10) business days and issue award or denial letters, via email, to applicants or participants. As part of this process the Schedule Contractor shall collect:*
   a. Furnish OPM 1643 CCS Application Form
   b. OPM 1644 Childcare Provider Information for the CCSP for Federal Employees
   c. Most recent SF-50
   d. Most recent income tax return for each parent/spouse or partner/guardian
   e. Two most recent pay stubs for each parent/spouse or partner/guardian
   f. Copy of the childcare provider's business license
   g. Copy of the childcare provider's fee schedule
   h. Proof of dependent child
      - **Childbirth**
        ✓ Birth Certificate

- ✓ Documentation provided by the employee's healthcare provider
- ✓ Document naming employee as second parent, such as declaration of paternity/court order of filiation
- ✓ Documentation provided by the child's healthcare provider
- ✓ Hospital admission form associated with the delivery

- **Adoption**
  - ✓ Documentation provided by the adoption agency confirming the placement and date of placement
  - ✓ Letter signed by parent's/parents' attorney confirming the placement and date of placement
  - ✓ Immigrant visa for the child issued by the U.S. Citizenship and Immigration Services
  - ✓ Adoptive placement agreement
- **Foster Care**
  - ✓ Foster care placement record
  - ✓ Other documentation from the foster agency confirming the placement and date of placement
  - ✓ Foster care placement letter issued by the relevant local department of social services or authorized voluntary foster care agency.

i. Any other documents required by DHS FEMA

3. *The Schedule Contractor must have an available system to allow applicants to apply and recertify online.*
4. *The Schedule Contractor's systems must have the ability to allow the applicants the ability to submit applications and recertification documents 24 hours a day.*
5. *Ability to generate ad-hoc reports.*
6. *Ability to host DHS FEMA materials with restricted access.*
7. *The Schedule Contractor's existing cloud-based platform shall be in accordance with Appendix A.*

4.0 CCSP ADMINISTRATION, EXECUTION, PROMOTIONAL MATERIALS AND ACTIVITIES CONTRACTOR REQUIREMENTS

A) The Schedule Contractor shall provide start-to-finish services, performing all necessary tasks to receive, process, and report subsidy payments in a streamlined and cost-efficient manner to include the following services:

1) Support DHS FEMA with the finalization of their specific agency guidelines and subsidy schedule(s).
2) Ensure applicants meet agency employment and salary thresholds.
3) Ensure childcare providers are licensed and have verified taxpayer ID numbers.
4) Ensure children are under the age of 13 or, if disabled, under the age of 18. Proof of disability documentation will be requested with the registration documentation. or under the age of 18, if disabled.
5) Ensure Schedule Contractor staff are available by telephone and email Monday to Friday 9am to 8pm EST to answer questions from FEMA CCSP Program Participants.
6) Respond to all employee questions within two (2) business days.
7) Generate and email monthly invoices for each enrolled family and/or provider.
8) Receive and process signed monthly invoices for each enrolled family.
9) Issue monthly Automated Clearing House (ACH) payments (or checks) to the childcare provider(s) based on the allowed subsidy for each participating family. Payments are processed within ten (10) business days of signed invoice receipt.
10) Email requests for recertification documents annually to all current participants to verify continued eligibility.

11) Mail reminders to the childcare provider when childcare provider license is about to expire. Reminders shall be sent within sixty (60) days of license expiration date.
12) Receive and process periodic updates to childcare provider licenses and information.
13) Receive and process change of provider forms.
14) Email notification when a participant reaches the annual subsidy cap (if applicable) in accordance with the CCSP guidelines in section 2.0.
15) Provide annual Form 1099 - MISC to childcare providers, as needed.
16) Maintain a wait list of employees when the program is full. Email employees on the wait list when enrollment reopens.
17) Maintain confidentiality of all information related to the CCSP.
18) Maintain program documentation in an electronic format that meets FedRAMP and HIPAA standards.

B) The Schedule Contractor shall create and provide on-going promotional materials to enhance awareness of CCSP to DHS FEMA employees that encourages utilization. As part of this process, the Schedule Contractor shall:

1. Provide on-going advertising and promotional materials in electronic and reproducible format throughout the performance period.
   a. Promotional materials include, but are not limited to, flyers, brochures, posters, and webinars.
   b. Promotional materials will include access instructions and a statement about participant eligibility.
2. Create and provide a kick-off campaign within thirty (30) calendar days after award.
3. Conduct two (2) live webinars within the performance period.
4. Work with the COR to customize promotional materials with DHS FEMA branding, including the agency and office name and logos.
5. Work with the COR to establish a strategy and timeline for updating promotional materials.

5.0 PERIOD OF PERFORMANCE:

The ordering period of performance for each of the CLINS mentioned above are:

CLIN 0001	**Childcare Subsidy Program Payments NTE 29 Participants January-September 2025**	**9 months**
CLIN 0002	**Service Charge Basic Fee NTE 199 Participants September 2024-September 2025**	**12 months**
CLIN 0003	**Childcare Subsidy Program Payments NTE 170 Participants January-September 2025**	**9 months**

6.0 PLACE OF PERFORMANCE:

The place of performance for this requirement shall be performed at the Schedule Contractor's facilities. The Schedule Contractor administrative/project management staff shall be available Monday to Friday 9am to 6pm EST to assist / answer questions and provide technical assistance.

7.0 DELIVERABLES

At a minimum, the Government requires the following documents as the deliverables. In addition, the Schedule Contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for the resultant BPA and its subsequent BPA calls. The content and format will be mutually agreed upon by the Schedule Contractor and DHS FEMA program office.

The presentation of deliverables, which includes texts, briefings, and any charts or other graphics shall be formatted as follows:

1. Marked with DHS FEMA logo and header.

2. Text may be formatted in any of the commonly available word processing programs marketed by the IBM®, Corel®, or Microsoft® corporations.
3. Provide a single file that contains the whole document ready for printing. It should reproduce the printed report exactly.
4. Tables and tabular material shall not be converted into graphical images but be included with the word processing files or delivered as spreadsheet files (Excel®).
5. Graphic figures such as bar and line charts, diagrams, and other drawings if required, shall be delivered in the GIF (Graphics Interchange Format) or the JPEG (Joint Photographic Experts Group) format. Graphical elements may be merged with the text to form a single file for printing purposes, or they may be delivered as separate files.
6. Adobe's Portable Document Format (PDF®) if required may not be substituted for the above word processing formats. An unlocked, PDF version may be provided in addition to the word processing version, but it is not required. Provide presentations, such as PowerPoint®, as separate file.

Item	Deliverable (D) Milestone (M)	Due Date	Method Of Delivery	Government Contractor Template Material
1	Provide/Maintain a Cloud Based CCS platform, (D)	Interim Operational Capability Cloud Based platform upon award Full Operational Capability upon successful attainment of Authorization Decision milestone (#11)	Cloud Based Platform	Contractor Platform
2	CCS Program Administration (M) Process New Applications (M)	On-Going Within 10 business days of Full Operational Capability of the cloud-based childcare subsidy platform and ongoing	Electronic copy	Schedule Contractor Form
3	Promotional Materials and Activities (D)	30 calendar days after award and ongoing	Electronic copy	Schedule Contractor Form
4	Kickoff Meeting (M)	14 calendar days after award	N/A	Schedule Contractor Form
5	Monthly Status Reports (D)	Monthly 10th calendar day of each month	Electronic copy	Schedule Contractor Form
6	Implementation Plan (D)	Draft Implementation Plan due upon receipt of quote. Final Implementation Plan due 14 calendar days after award.	Electronic copy	Schedule Contractor Form

7	Outgoing Transition Plan (D)	Initial draft 30 days after award. Final draft due 60 calendar days prior to the end of the base and any option period, unless otherwise directed by the CO.	Electronic copy	Schedule Contractor Form
8	BPA Activity Meeting	Monthly or as needed	N/A	N/A
9	Meeting Minutes	Monthly or as needed	Electronic copy	Schedule Contractor Form
10	IT Systems Security Plan	Submit at the time of proposal	Electronic copy	Schedule Contractor Form
11	DHS FEMA Authorization Decision (M)	Within 365 days of Task Order Award	Electronic copy	Government Form
12	Section 508 Test Plans	TBD	Electronic copy	Schedule Contractor Form
13	Section 508 Test Results	TBD	Electronic copy	Schedule Contractor Form
14	Section 508 Accessibility Conformance Reports	Upon Request	Electronic copy	Government Form (Identified in Section 9.2.3)
15	Other Section 508 Documentation	Upon Request	Electronic copy	Schedule Contractor Form
16	Security Document Destruction Plan	Submit within 180 days of BPA award	Electronic copy	Schedule Contractor Form
17	Provide access to non-production platform/service to allow for training and user guide creation	10 days after award	Electronic copy	Schedule Contractor Form

8.0 KICK-OFF MEETING

No later than fourteen (14) business days after the effective date of the award, key members (as designated by the Schedule Contractor) of the Schedule Contractor's staff who will be assigned major responsibility for carrying out the tasks of the Task Order shall meet with the Contracting Officer (CO), COR, and other interested government personnel within DHS FEMA in a Microsoft Teams meeting. This meeting will ensure the Schedule Contractor and the Government have a common understanding; in addition, they will discuss the project's objectives, planned course of action, milestones and deliverables, and resolve any differences between the technical requirements and the Schedule Contractor's approach. The Schedule Contractor shall first conduct a briefing (i.e. 30–45 minutes) describing the firm's approved approach. The Schedule Contractor shall be prepared with appropriate briefing materials.

9.0 MONTHLY STATUS REPORTS

The Schedule Contractor shall on or before the 10th calendar day of each month by 3:00 PM EST submit the Monthly Status Report to the COR electronically. Each report shall summarize activities for the preceding month, to include:

- number of employees that applied

- number of employees denied due to exceeding the cap
- key thematic questions employees have been asking
- number of employee complaints and adjudication
- total number of subsidies
- processed work accomplished and problems solved
- work planned (present and anticipated challenges, issues or problems)
- expenditure rate with corresponding roll up to major task component;
- and any other pertinent issues, as well as identified significant work-ahead for the next reporting period.

The format should be in Microsoft (MS) Suite to include MS Word, MS Excel, MS PowerPoint, MS Access or Adobe Acrobat (PDF). Should the 10th day of the month fall on the weekend or Federal holiday, the report is to be submitted the first Federal workday preceding the weekend or Federal holiday.

At a minimum, this report shall include a narrative description of the following items:
- Accomplishments made during the reporting period
- Plans for accomplishments in next reporting period
- A review of the overall progress in the conduct of this BPA
- Problems or delays that the Schedule Contractor has experienced in the conduct of services
- Specific action that the Schedule Contractor would like DHS FEMA to undertake to help alleviate identified problem
- Invoices submitted and paid out to participants during the reporting period
- Enrollment status to include the number of eligible participants and ineligible participants with the reason for permanent or temporary ineligibility.
- Application queue status to include the number of received, in-process, approved, approved awaiting award return and denied applications with the reason for denial.

10.0 IMPLEMENTATION PLAN

The Schedule Contractor shall provide fourteen (14) calendar days after Task Order award a detailed Implementation Plan that includes phase-in and phase-out procedures for services, products, and deliverables required under this SOW. The Implementation Plan's incoming (phase-in) activities shall include:

1. Transferring work to the incumbent Schedule Contractor
2. Potential problems and mitigation plans.
3. Assumption of full BPA responsibilities.
4. Transferring of documentation and projects currently in process.
5. Document all current work and processes.
6. Coordinate the work with the new and/or existing Schedule Contractor.

The Schedule Contractor shall make all necessary preparations to begin BPA performance in accordance with its Implementation Plan in order to ensure no impact to daily operations or scheduled critical activities.

11.0 OUTGOING TRANSITION ACTIVITIES

The Outgoing Transition Plan shall be submitted thirty (30) calendar days after Task Order award. The Outgoing Transition Plan will include draft phase-out transition activities for all transition effort for follow-on requirements for minimize disruption of services. The Schedule Contractor shall work with the new Schedule Contractor to provide knowledge transfer and transition support as required by the COR. The Transition Plan's phase-out activities and support shall include:

1. Coordination with Government Representatives.
2. Review, evaluation, and transition of current support services.
3. Transfer of all necessary business and/or technical documentation in electronic formats.
4. Inventory and return all Government Furnished Information (GFI) in Schedule Contractor possession.
5. Provide report on status of all deliverables.
6. Provide report on problems encountered during period of performance.
7. Provide report on current issues, problems, or activities in process that require immediate action.
8. Provide the plan on how the Schedule Contractor intends to transition follow-on requirements, and the list of key personnel involved in this effort.
9. Final deliverables that are due.
10. Applicable debriefing and personnel out-processing procedures.
11. Identify and provide a schedule of routine events for continuity of program (e.g., reports and processes).

Updates to the Outgoing Transition Plan to finalize phase-out transition activities are due sixty (60) calendar days prior to the end of the base and any option period, unless otherwise directed by the CO. The COR shall review phase-out transition activities within five (5) calendar days after receipt. Upon government approval of the phase-out transition activities, the Schedule Contractor shall execute the phase-out transition support to commence six (6) months prior to the expiration of this Task Order.

12.0 BPA ACTIVITY MEETING

The COR shall convene a monthly meeting or more frequently, as needed, to discuss BPA activity with the Schedule Contractor's designated point of contact (POC). This will ensure that all participants are well-informed and up to date on all activities and are provided an opportunity to identify other activities and establish priorities, as well as coordinate resolution of identified problems.

13.0 MEETING MINUTES

The Schedule Contractor shall provide minutes of meetings including attendance, issues discussed, decisions made, and action items assigned, to the COR electronically within five (5) business days following each meeting conducted with the Government.

14.0 IT SYSTEMS SECURITY PLAN

The Schedule Contractor shall submit written proof of IT Security accreditation as part of the proposal of this Task Order. Accreditation will proceed according to the criteria of DHS FEMA Policy Directive 4300A: Information Technology System Security Program, Sensitive Systems, or any replacement publication. This accreditation will include a final security plan, risk assessment, security test and evaluation, disaster recovery plan, and continuity of operations plan. This accreditation, when accepted by the Government, shall be incorporated into the BPA as a compliance document. The Schedule Contractor shall comply with the approved accreditation documentation. The Schedule Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS FEMA network or operated by the Schedule Contractor for DHS FEMA, regardless of location. This applies to the Schedule Contractor's entire enterprise information technology architecture and any information technology resources or services for which the Schedule Contractor must have physical or electronic access to sensitive information contained in DHS FEMA unclassified systems.

The Schedule Contractor shall provide, implement, and maintain an IT System Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of all systems operated and maintained in the performance of this BPA.

The Schedule Contractor shall, within thirty (30) calendar days after the post-award conference, provide for approval its IT System Security Plan to the BPA PM and BPA COR. The Schedule Contractor's approved IT System Security Plan shall be incorporated into the BPA as a compliance document.

The Schedule Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), the Government Information Security Reform Act of 2000, and the Federal Information Security Management Act of 2002, and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.
The Schedule Contractor's IT Security Plan shall specifically include instructions regarding handling and protecting sensitive information at the Schedule Contractor's site (including any information stored, processed, or transmitted using the Schedule Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions includes:
1. Acquisition, transmission, or analysis of data owned by DHS FEMA with significant replacement cost should the Schedule Contractor's copy be corrupted, and
2. Access to DHS FEMA networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall)

At the expiration of the BPA, the Schedule Contractor shall return all sensitive DHS FEMA information and IT resources provided to the Schedule Contractor and certify that all non-public DHS FEMA information has been purged from any Schedule Contractor-owned system. DHS FEMA Components shall conduct reviews to ensure that the security requirements in the BPA are implemented and enforced.

15.0 SECTION 508 DELIVERABLES

15.1 SECTION 508 TEST PLANS

When providing ICT pursuant to this contract, the Schedule Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the life cycle of the BPA, who will conduct the testing, how test results will be reported, and any key assumptions.

15.2 Section 508 Test Results

When providing ICT pursuant to this contract, the Schedule Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

15.3 Section 508 Accessibility Conformance Reports

For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are provided pursuant to this contract), the Schedule Contractor shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

15.4 Other Section 508 Documentation:

The following documentation shall be provided upon request for ICT items offered through this BPA:
1. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
2. Documentation on how to configure and install the ICT Item to support accessibility.

3. Documentation of core functions that cannot be accessed by persons with disabilities.

16.0 SECURITY DOCUMENT DESTRUCTION PLAN

The Schedule Contractor shall submit a plan for destruction of the retained sensitive data within 180 calendar days after receipt of award. The Schedule Contractor shall retain the information up to at least one (1) year online and up to at least three (3) years offline.

The Schedule Contractor must complete the following required security documents within 180 calendar days after receipt of award:

1. Requirements Traceability Matrix
2. Contingency Plan
3. Contingency Plan Test

17.0 PROTECTION OF GOVERNMENT FURNISHED INFORMATION

The Government will provide GFI within seven (7) business days after the Task Order award along with guidelines that determine the eligibility and subsidy distribution. Schedule Contractor access to information protected under the Privacy Act is required thereunder the BPA contract. Schedule Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

18.0 INTELLECTUAL PROPERTY

All intellectual property resulting from activities undertaken in performance of this BPA and any resultant BPA calls shall be governed under the applicable FAR patent and data rights clauses incorporated therein the BPA contract, including FAR 52.227-1, 52.227-2, and FAR 52.227-17, along with any special BPA contract requirements prescribed therein Section H that relate to data and patent rights.

19.0 SECURITY

Schedule Contractor access to unclassified, but security sensitive information, may be required under this BPA. Schedule Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

The work under this SOW will be unclassified. All Schedule Contractor employees shall be required to complete a Non-Disclosure Agreement (DHS FEMA Form 11000-6) within two (2) business days after award; or prior to performing any work on this Task Order.

20.1 Contract Personnel Security

Personnel may 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 FEMA 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: 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 FEMA Management Directive 11042.1 contractors, consultants and others to whom access is granted will abide by 11042.1; DHS FEMA policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS FEMA. It also applies to other sensitive but unclassified information received by DHS FEMA 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 FEMA 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 FEMA, 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 FEMA Policy and not applied retroactively.

Foreign Travel and Government-Issued Equipment:
Per DHS FEMA 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 FEMA or FEMA information systems, routine access to DHS FEMA 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 FEMA 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 FEMA 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 FEMA Form 11000-6, "Non-Disclosure Agreement"
- DHS FEMA 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 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 have 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 FEMA 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 FEMA- or FEMA-issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS FEMA or FEMA may subject the contractor personnel and the Contractor to civil and criminal liability.

20.1.1 Homeland Security Presidential Directive 12 (HSPD-12) Information

20.1.1.1 Procurements for products, systems, services, hardware, or software involving controlled facility or

information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
20.1.1.2 Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and Schedule Contractors.
20.1.1.3 PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
20.1.1.4 If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the DHS FEMA Chief Information Security Officer (CISO).
20.1.1.5 The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS FEMA facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS FEMA sensitive systems. The Schedule Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS FEMA resources to include IT applications and physical facility.
20.1.1.6 The DHS FEMA Office of the Chief Security Officer shall be notified of all terminations/resignations within five (5) days of occurrence. The Schedule Contractor shall return to the Contracting Officer Representative (COR) all DHS FEMA issued Personal Identity Verification (PIV) credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card. The Contractor or contractor personnel's failure to return all DHS FEMA issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the BPA, or upon demand by DHS FEMA may subject the Schedule Contractor personnel and the Schedule Contractor to civil and criminal liability.

20.2 CONTRACTOR EMPLOYEE IDENTIFICATION

The Schedule Contractor shall ensure that its personnel identify themselves as Schedule Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

20.3 CONTRACTOR PERSONNEL

The Schedule Contractor shall at all times maintain an adequate workforce to ensure uninterrupted performance of all tasks defined within this SOW.

20.4 TRAVEL

No travel is anticipated under this SOW.

20.5 CHANGES TO THE SOW

No changes to the resulting SOW or cost increases shall be incurred without written prior approval of the CO as coordinated by the COR. Any changes or cost increases will not take effect until the CO executes a written modification.

20.6 QUALITY CONTROL

The Contractor shall employ its commercial quality control program/procedures to identify, prevent, and ensure non-recurrence of defective services. Through implementation of the Contractor's quality control

program/procedures, the Government shall receive quality services meeting the requirements of this contract.

20.7 APPLICABLE DOCUMENTS OR REFERENCES

See Appendix A, Reference Document.

Appendix A- Applicable Documents and References

INFORMATION SYSTEM SECURITY COMPLAINCE- AUTHORIZATION DECISION (AD)
The Schedule Contractor shall not input, store, process, output, and/or transmit sensitive information within a Schedule Contractor information technology system without an Authorization Decision signed by the DHS FEMA Headquarter or DHS FEMA Component Chief Information Officer (CIO), or designee, in consultation with the DHS FEMA Headquarter or DHS FEMA Component Privacy Officer. Unless otherwise specified in the Authorization Decision, the Authorization Decision is valid for one (1) year. The Schedule Contractor shall adhere to current and updated federal and DHS FEMA-specific policies, procedures, and guidance for the Security Authorization (SA) process as defined in https://www.DHS FEMA.gov/publication/security-training-contract-policy and NIST Special Publication 800-37, Revision 2, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, January 2020.

The Schedule Contractor's Information System Security Officer (ISSO) shall coordinate all security activities with the Federal ISSO and/or System Owner. The Portfolio Management Division Information System Security Manager (ISSM) will provide guidance to the Federal ISSO for management with the Schedule Contractor ISSO where needed.
All information technology and security compliance documents shall be submitted to the Contracting Officer's Representative (COR) and reviewed and approved by the DHS FEMA Chief Information Security Office Directorate (CISOD) upon creation and after any subsequent changes before they go into effect. All security documentation and artifacts will be uploaded and documented in the DHS FEMA system of record.

DHS FEMA ENTERPRISE ARCHITECTURE COMPLIANCE
The cloud-based interface and services shall meet DHS FEMA Enterprise Architecture policies, standards, and procedures. Specifically, the Schedule Contractor shall comply with the following Homeland Security (HLS) Enterprise Architecture (EA) requirements:

1. All provided deliverables and requirements shall be compliant with the HLS EA;
2. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile;
3. 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 FEMA Data Reference Model and Mobius;
4. Development of data assets, information exchanges and data standards will comply with the DHS FEMA Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS FEMA data management architectural guidelines;
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS FEMA-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS FEMA 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. The Schedule Contractor shall utilize and adhere to the DHS FEMA Enterprise Security Architecture to the best of its ability and to the satisfaction of the Government. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers;
2. Compliance to DHS FEMA Identity Credential Access Management (ICAM);
3. Security reporting to DHS FEMA central control points (i.e., the DHS FEMA Security Operations Center (SOC) and integration into DHS FEMA Security Incident Response;
4. Integration into DHS FEMA Change Management (for example, the Infrastructure Change Control Board (ICCB) process);
5. Performance of activities per continuous monitoring requirements

The Schedule Contractor shall participate in DHS FEMA's Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that DHS FEMA determines acceptable. The DHS FEMA Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the Schedule Contractor shall implement and maintain the following processes in accordance with the NIST Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations (https://csrc.nist.gov/publications/detail/sp/800-137/final):

11. Asset Management
12. Vulnerability Management
13. Configuration Management
14. Malware Management
15. Log Integration
16. Security Information Event Management (STEM) Integration
17. Patch Management
18. Provie application event logs to the DHS FEMA Security Operations Center (SOC)
19. Near-real-time security status updates to the DHS FEMA SOC

The Schedule Contractor shall comply with requests to be audited and provide responses within three (3) business days to requests for data, information, and analysis from DHS FEMA and any applicable Component COR. The Schedule Contractor shall provide support during the audit activities and efforts. These audit activities may include, but are not limited to, the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

DHS FEMA Application Architecture Compliance

The Schedule Contractor shall ensure that the application is designed for browser independence (i.e., the application will generally work with any of the major browsers). DHS FEMA HQ currently uses Microsoft Edge (Version 105.0.1343.50 (Official build) (64-bit)) configured with numerous Group Policy Objects (GPOs) as well as Firefox (102.3.0esr (64-bit)), similarly, secured with centrally managed security policies. Browser specific implementations or limitations on browser independence shall be approved in writing by DHS FEMA OCIO prior to development. Web Applications should be designed utilizing a responsive web design (RWD) approach, to provide an optimal viewing and interaction experience, independent of that platform capabilities the end user is utilizing. If DHS FEMA OCIO upgrades to a newer version of Microsoft Edge or Firefox, the Schedule Contractor shall ensure the application is compatible with the future version.

DHS FEMA OPEN-SOURCE COMPLIANCE

The Schedule Contractor shall follow the DHS FEMA Reusable and Open-Source Software Policy Directive (Policy Directive 142-04) when evaluating any technologies, tools, software, and/or application programmable interfaces (APIs) to support a system.

FEDRAMP CERTIFICATION COMPLIANCE

The Schedule Contractor's enterprise architecture shall be hosted on a FedRAMP authorized, cloud-based software as a solution (SaaS), or in one of the DHS FEMA cloud-based environments. At a minimum, the Schedule Contractor's enterprise architecture shall have a moderate impact level.

CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

1. Definitions

a. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.

b. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

c. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

d. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

e. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

2. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product.

a. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.

b. The contractor may provide previously used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

3. Accounting of Components in ICT Products

a. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.

b. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

c. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract and replaced when End of Support (EoS) is reached.

d. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

4. Supply-Chain Transport

a. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.

b. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance and make available for inspection upon request of the Government.

c. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.

d. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

e. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

5. Changes to Ownership and Control

6. The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

Applicable Documents and References

The Government requires the Schedule Contractor to adhere to and follow all applicable executive orders, presidential directives, federal laws, and DHS FEMA management policies, handbooks, guidelines, processes, and procedures:

1. DHS FEMA Policy Directive 4300A: Information Technology System Security Program, Sensitive Systems, v13.3;

2. Department of Defense (DoD) Manual 5200.01 Volumes 1-3, February 24, 2012;

3. Office of Personnel Management - Enterprise Human Resources Integration (EHRI):

4. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/enterprise-human- resources-integration/ ;

5. https://www.opm.gov/policy-data-oversight/data-analysis-documentation/data-policy- guidance/#url=Data-Reporting-Guidance ;

6. The National Institute of Standards and Technology (NIST) serve as the proponent for cybersecurity guidance and publishes the Cybersecurity Framework for the federal sector. Within this framework, NIST SP 800-53 Rev. 5, September 2020 is the common document used to reconcile security controls. Federal Information Security Modernization Act (FISMA) mandates the following NIST guidance and standards:

6.1 Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

6.2 FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006

6.3 Special Publication 800-37 Rev. 2, Risk Management Framework for Information Systems and

Organizations: A System Life Cycle Approach for Security and Privacy, December 2018
6.4 Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
6.5 Special Publication 800-53A Rev.5, Assessing Security and Privacy Controls in Information Systems and Organizations, January 2022
6.6 Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, August 2003
6.7 Special Publication 800-60 Vol.1 Rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
6.8 NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization, December 2014
6.9 NIST SP 800-144, Guidelines of Security and Privacy in Cloud Computing, December 2011
6.10 NIST SP 800-146, Cloud Computing Synopsis and Recommendations, May 2012
6.11 Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, March 2019
7.DHS FEMA Directive 140-01 Rev. 2, Information Technology Security Program, May 2017
8.DHS FEMA Instruction Guide 040-01-008, Privacy Incident Handling Guidance, December 2017
9.DHS FEMA Security Authorization Process Guide
10. DHS FEMA Management Directive 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, January 2015
11. DHS FEMA Instruction Handbook 121-01-007, Personnel Suitability and Security Program, February 2019
12. Coast Guard Cybersecurity Manual, Commandant Instruction (COMDTINST) M5500.13 (series) – FOUO
13. DoD Instruction (DODI) 8500.01, Cybersecurity, October 2019
14. DODI 8510.01, Risk Management Framework for DoD Systems, July 2022
15. DODI 8520.03, Identity Authentication for Information Systems, May 2023
16. DODI 8530.01,Cybersecurity Activities Support to DoD Information Network Operations, July 2017
17. DoD Cloud Computing Security Requirements Guide (SRG), Version 1, Release 3, March 6, 2017
18. Defense Information Systems Agency (DISA) Cloud Connection Process Guide, Version 2, March 2017
19. CJCSM 6510.01B, Cyber Incident Handling Program, Chairman of the Joint Chiefs of Staff Manual (CJCSM), December 2014
20. Information Assurance Vulnerability Management - DOD CJCSI Policy 6510-01F, Assurance (IA) and Computer Network Defense (CND), and CJCSM 6510-01B Cyber Incident Handling Program. National Security systems guidance can be found at https://www.cnss.gov/CNSS/issuances/Policies.cfm.
21. Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001
22. PDD 63, Critical Infrastructure Protection, May 1998
23. DoD Memorandum for Cybersecurity Activities Performed for Cloud Service Offerings, November 15, 2017
24. DHS FEMA Policy Directive 142-04, DHS FEMA Reusable and Open-Source Software Rev. 01, August 2021
25. Federal Employees' Health, Counseling, and Work/Life Programs // Agency Use of Appropriated Funds for Childcare Costs for Lower Income Employees, 5 CFR Part 792, Subpart B;
26. Appropriated Amounts for Affordable Childcare, 40 USC 590(g)
27. Federal Cloud Computing Strategy, February 2011;
28. Security Authorization of Information Systems in Cloud Computing Environments, December 2011;
29. 25 Point Implementation Plan to Reform Federal Information Technology, December 2010;
30. HSPD-12 – Policies for a Common Identification Standard for Federal Employees and Contractors;
31. OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors";

32. OMB M-06-16 – Acquisition of Products and Services for Implementation of HSPD-12; and
33. NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

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 Pub. L. 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 FEMA 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), 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 improper information modification or 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 FEMA policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.DHS FEMA.gov/DHS FEMA-security-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 FEMA Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems.* If the Component SOC is not available, the Contractor shall report to the DHS FEMA Enterprise SOC. Contact information for the DHS FEMA
Enterprise SOC is accessible https://www.DHS FEMA.gov/DHS FEMA-security-and-training-requirements-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 FEMA 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 FEMA 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 FEMA 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 FEMA 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.

(End of clause)

3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) *Definitions.* 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 FEMA 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.

(1) 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.

(2) 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:
(i) Truncated SSN (such as last 4 digits);

(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) 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.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction 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 or 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, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements*. The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the 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.

(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 FEMA, as appropriate), and other key metrics; (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS FEMA, as appropriate;
(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

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 FEMA: Protecting Personal Information accessible at http://www.DHS FEMA.gov/DHS FEMA-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)

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

(End of clause)

INFORMATION SHARING
To accomplish the tasks outlined in this contract, FEMA will provide the contractor access to the PII and SPII

for the employees and family members such as name, phone number, home address, email address, bank account etc.

The information sharing outlined in this contract is authorized by the following System of Records Notice(s) and Routine Use(s):

DHS FEMA/ALL-007 Accounts Payable System of Records, December 21, 2018, 83 FR 65705
DHS FEMA/ALL-012 Department of Homeland Security Childcare System of Records, October 3, 2008, 73 FR 57642 (Routine Use F)

The information sharing outlined in this contract is authorized by the following Privacy Impact Assessments:

DHS FEMA/ALL/PIA-096 Employment Verification and Unemployment Compensation (January 11, 2023)
DHS FEMA/ALL/PIA-066 DHS FEMA Employee Assistance Program (June 11, 2018)

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.

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.