+

Federal Emergency Management Agency (FEMA)

Grants Management Modernization (GMM) Program
Agile Development (GMMAD) Services
Blanket Purchase Agreement (BPA)
Performance Work Statement

Performance Work Statement
GMM Agile Development Services

I. Background

The Federal Emergency Management Agency (FEMA) Grants Management Modernization (GMM) Program is an initiative which seeks to simplify and coordinate business management approaches across all the Agency's 40+ grants programs. GMM is establishing a common grants life cycle and platform for users with the new system called FEMA Grants Outcomes (FEMA GO).

The GMM Program is a user-centered, business-driven approach which engages with stakeholders to fully capture modernization needs, gaps, and transformation opportunities. Streamlined grants processes are derived from common business processes to achieve a unified technology platform. The GMM cross-agency and integrated approach improves the oversight and monitoring of funding allocations and support integrated data analytics across the program areas for improved efficiencies.

GMM consolidates FEMA's legacy grants IT systems into a single grants management IT platform. The program also consolidates FEMA's grants operations, establishing a common grants management lifecycle and unifying business processes across grant programs where possible. These changes improve the efficiency and effectiveness of FEMA's grants operations, thereby strengthening the Agency's ability to carry out its mission.

II. Purpose

GMM seeks to establish a multiple-award blanket purchase agreement (BPA) for acquiring technical services needed to continue the development efforts relating to the FEMA GO system. This Agile development effort is in direct support of the FEMA mission, and it is intended to support operations without disruption of existing application functionality.

Orders under the multiple-award BPA shall provide Agile development activity, code delivery for functionality, and related services. New, unplanned requirements may result from disasters or legislative actions and may be to support either new or legacy FEMA grants programs.

III. Scope

GMM has a continuing need for software code development for the FEMA GO system. Contractor resources shall support the GMM program by adapting FEMA GO to new requirements and delivering software for capability that was deferred until after Full Operational Capability (FOC). Development services shall be provided to GMM using the Agile software development methodology. Agile development services shall apply design and engineering best practices to implement a modular, scalable, resilient application that fully integrates in the

FEMA enterprise and completely interoperates with other FEMA applications, and which is in compliance with DHS and FEMA Enterprise Architecture (EA) and Cyber Security directives and policies. New, unplanned requirements that are addressed may result from disasters or legislative actions and may be to support either new or legacy FEMA grants programs.

The Contractor shall provide Agile development activity, code delivery for functionality, and related services (e.g. design). Requirements may include planned work, such as capability deferred until after FOC, that is included in the GMM Life Cycle Cost Estimate (LCCE) and unplanned work required for new and legacy FEMA grants programs that are funded from other FEMA sources. New requirements that may result from disasters or legislative actions and be to support either new or legacy FEMA grants programs may not yet be as well defined or known in as great of detail as other requirements, such as planned work for capability deferred until after FOC.

The Contractor shall perform to the standards outlined. The Contractor shall ensure all services are provided efficiently and economically, while providing quality products and services meeting customer requirements. The performance metrics utilized shall ensure all standards are met as in the summarized in the Performance Requirements Summary (PRS) section of this PWS. The government has aligned its Quality Assurance Surveillance Plan (QASP) to monitor the key indicators in the contractor's PWS that effect these standards.

The Contractor shall assist in further developing software code necessary for the integration of the Hazard Mitigation Assistance, Individual Assistance, Public Assistance and the Environmental and Historical Preservation program requirements, and any other FEMA grant program as requested by FEMA. In this capacity, the Contractor shall apply design and engineering best practices to implement a modular, scalable, resilient application that fully integrates in the FEMA enterprise and completely interoperates with other FEMA applications, and which is in compliance with DHS and FEMA Enterprise Architecture (EA) and Cyber Security directives and policies. In addition, the Contractor shall prepare and maintain any applicable Acquisition Lifecycle Framework (ALF) and Systems Engineering Life Cycle (SELC) documentation.

Primary Place of Performance is determined at the call order level, unless otherwise agreed upon.

With COR approvable, telework is allowable. Otherwise, Place of Performance may be at the Contractor's facilities or FEMA facilities, including FEMA Headquarters in Washington, DC 400 C Street SW, Washington DC, 20472

The Period of Performance (POP) of the multiple-award BPA shall be a base period of date of award for one (1) year and four (4) one year option periods.

The contract types of the orders allowed shall be firm-fixed-price (FFP), Labor Hour (LH) / Time and Material (T&M), or hybrid of the former types.

Hours of Operation may be established at the call order level. Contractor employees shall generally perform all work between the hours of 07:00 AM and 05:00 PM ET, Monday through

Friday. However, due to the response FEMA has for disaster activities, there may be occasions when contractor employees shall be required to work other than normal business hours, including evenings, weekends, and holidays, to fulfill requirements under this SOO. Any work required after normal hours, including overtime, must be approved in writing by the Contracting Officer or Contracting Officer's Representative before it occurs.

IV. Applicable Documents and Definitions

1. DHS Directive: 102-01-001 (or latest) and it's implementing Instructions.
2. DHS Directive: 102-01-103 - Appendix B - SYSTEMS ENGINEERING LIFE CYCLE
3. DHS Instruction Guide 026-06-001-01 Test and Evaluation Master Plan (TEMP)
4. GMM Program Documentation:
    i. Mission Needs Statement (MNS)
    ii. Concept of Operations (CONOPs)
    iii. Integrated Logistic Support Plan (ILSP)
    iv. Analysis of Alternatives (AoA)
    v. Operational Requirements Document (ORD)
    vi. Test and Evaluation Master Plan (TEMP)

Defect Level	Definition Of Defect Categories	Defect Category
1	• Prevents the accomplishment of an essential capability • Jeopardizes safety, security posture, or any other requirement designated as critical	Critical
2	• Adversely affects the accomplishment of an essential capability and no acceptable system workaround exists • Aggravates technical, cost, or schedule risk to the project or to life cycle support of the system and no acceptable system workaround exists	Major
3	• Adversely affects the accomplishment of an essential capability and an acceptable system workaround exists • Increases technical, cost, or schedule risk to the project or to life cycle support of the system and an acceptable system workaround exists	Moderate
4	• Results in an inconvenience to the user or operator but does not affect a required operation of mission critical capability • Results in an inconvenience for development or maintenance personnel but does not prevent the accomplishment of the responsibilities of the personnel	Minor
5	• Enhancements to system or defects that may be deferred without resulting in an inconvenience to the user, operator, development personnel, or maintenance personnel	Minimal

V. Ordering

The Contracting Officer shall send each request for call order proposal by email to the Contractor. Each request for call order proposal shall specify whether the requirement is FFP, LH, or a hybrid of FFP and LH. Call order proposals shall be scoped as FFP, LH, or hybrid of FFP and LH accordingly. Unless otherwise agreed to by the Contracting Officer and the Contractor, the Contractor shall respond to each request for call order proposal with any questions within 3 business days. Unless otherwise agreed to by the Contracting Officer and the contractor, the contractor shall submit a proposal within 7 business days of receiving answers to questions or within 7 business days of the initial request for call order proposal if no questions are submitted. Call order proposals may offer rates or a basis of estimate further discounted below the established rates of the BPA. However, call order proposals shall not exceed the established rates of the BPA. Evaluation criteria and factors shall be within the scope of the BPA and established at the call order proposal request level.

VI. Tasks Areas

This BPA includes the following functional areas:

- Project Management Services
- Agile Development support to FEMA GO

6.1 **Task 1**: Project management services.

At the BPA level, the Contractor shall continue to maintain its accepted Project Management Plan (PMP) that was approved by the Government prior to award. The BPA-level PMP shall incorporate the Contractor's BPA-level Quality Control Plan, the Contractor's BPA-level Change Management Plan, and the Contractor's BPA-level Staffing Plan. Updates to the BPA-level PMP shall be submitted within one week of agreement, approval, or realization of the change.

As determined at the call order level, the Contractor shall manage its Agile development activity, provide project management services, and assess and report on performance.

As determined at the call order level, contractor tasks may include the Contractor being required to:

a. Manage its operations and teams.

b. Provide timely and comprehensive reporting on management, schedule, technical, and financial progress.

c. Meet with the Government no later than five (5) business days following award for a Post Award Kick-off to discuss project and expectations.

d. Continue to maintain accepted Project Management Plan (PMP) and operational model that demonstrates the overall management approach to meeting the requirements of the PWS and was approved by the Government prior to award. Updates to the PMP shall be submitted within one week of agreement, approval, or realization of the change. The PMP shall incorporate the Contractor's Quality Control Plan, the Contractor's Change Management Plan, and the Contractor's Staffing Plan.

e. Continue to maintain accepted Change Management Plan that has been incorporated into the call order. The Change Management Plan shall describe the processes and procedures for managing and documenting change requests and changes. The Change Management Plan shall be incorporated in the PMP.

f. Continue to maintain accepted Staffing Plan that has been incorporated into the call order. The Staffing Plan shall describe the Contractor's processes and procedures for identifying, recruiting, hiring, and retaining sufficient numbers of qualified, trained/certified personnel to meet stated Government objectives; the Contractor's processes and procedures for planning, resourcing, managing, and monitoring progress in meeting Government objectives; and the Contractor's ability to manage the magnitude and complexity of the order. The Staffing Plan shall include a staffing matrix, key personnel resumes, job/labor descriptions for each job/labor category title, and corresponding role(s) and responsibilities for each resource. The Staffing Plan shall demonstrate the technical qualifications, knowledge, and skills of personnel and how they correlate to the PWS requirements. Each job/labor category description shall include, at a minimum, information regarding the required education level, years of experience (expressed as a minimum number of years or as a range), and any other qualifications that are specifically required for performing the duties of the relevant job/labor category and role. The Staffing Plan shall be incorporated into the PMP and operational model.

g. Participate in or lead Agile and Program Management activities, including demos and sprint planning meetings, with GMM to demonstrate progress and current issues.

h. Update and maintain relevant program documentation and the Product Roadmap that incorporates projects, features, activities, and milestones necessary for the design, development, training and implementation of the GMM target solution. Activities include, but are not limited to, major acquisition decision events, systems engineering lifecycle reviews, design reviews to ensure that existing functionality in FEMA GO is being leveraged, testing events, security strategies, data solutions, training, and helpdesk.

i. Perform scheduled risk assessments to ensure data security and compliance with the established System Authority to Operate (ATO). Comply with FEMA and DHS security requirements.

j. Meet SELC requirements as specified in the GMM SELC Tailoring Plan and support the GMM in preparations for all gate, oversight, and governance reviews.

k. Present a monthly In-Progress Review (IPR) briefing to GMM that addresses program progress, cost/price, schedule, performance measurements, risks, technical issues, and management challenges.

l. Work with GMM to schedule and perform user research activities.

m. In support of GMM, develop, update, and maintain an Agile Dashboard that displays and tracks relevant metrics related to progress and performance.

n. In support of GMM reporting, track and report the following metrics:

    i. Deployment / Test Coverage
    Deployment refers to deployments to production. This metric indicates how often a program is deploying usable functionality. A higher frequency of deployments allows programs to respond to user feedback more quickly. A higher Deployment Rate is key for continuous delivery. Since smaller, more frequent deployments allow for faster delivery of value to the user and more feedback from users, this metric achieves the Agile outcomes of Increased Customer value and faster Time to Market.

    For Deployment/Test Coverage:
    1. Number of deployment to prod for each week in a month:
        A. Week 1
        B. Week 2
        C. Week 3
        D. Week 4
        E. Week 5 – when applicable
    2. Type of Deployment:
        A. Please select all that apply:
            (a) New Functionality
            (b) Maintenance
            (c) Patch
            (d) All
    3. % of Code Test coverage:
        A. This is the percentage of the code that is executed as part of an automated unit test suite. This metric indicates how much of a codebase has been tested.

ii. Availability

Availability is defined as the amount of time a system, application, or platform is operational in production. This metric indicates the stability and reliability of the system, application, or platform. It also highlights any disruption in service to users. A system that is stable and reliable helps to achieve the Agile outcome of Increased Customer Value.

For Availability, provide the availability for each system up/down date/time: (Note: For cloud purposes, any significant degradation of performance will be used to fulfill this metric in lieu of traditional server outages which are not applicable.)

1. System Down Date:
    A. This is the date the system went down.
2. System Down Time (EST):
    A. This is the time the system went down
3. System Up Date:
    A. This is the date the system came back up
4. System Up Time (EST):
    A. This is the time the system came back up
5. Total Downtime (Days: Hours: Minutes):
    A. This is the total period of time when a system is unavailable
6. Planned:
    A. Yes or No
7. Reason for Downtime:
    A. This is the reason the system went down. Please select one that applies:
        (a) Application Error
        (b) Network Outage
        (c) System Patching
        (d) System Release
        (e) Other (Please explain if this option is selected.)

6.2 **Task 2**: Agile development support to FEMA GO.

As determined at the call order level, the Contractor shall provide Agile development support, including the delivery of software functionality and code.

As determined at the call order level, contractor tasks may include but are not limited to the Contractor being required to:

a. Deliver software functionality and code in compliance with the Performance Requirements Summary and according to Roadmap Planning and Dev Done Planned dates, factoring in sufficient time for IV&V and UAT timelines, unless approved by the Government to deliver at another agreed upon date. Development activity and

code delivery shall be according to Roadmap Planning and consistent with the Contractor's approved Staffing Plan.

b. Provide technical capacity and development resources according to approved Staffing Plan that shall focus on the delivery of software functionality as determined by the GMM Product Owners. GMM Product Owners will determine development priorities on a quarterly basis, and the development team is expected to deliver according to the priorities agreed by the Product Owners during the Quarterly Product Roadmap Increment Planning sessions. If changes (configurations or updates) do not satisfy GMM Product Owners' customer needs, the Contractor shall add new stories to the backlog but shall not link them to the current delivery release.

c. Conduct design reviews on the front end to ensure FEMA is leveraging existing functionality in FEMA GO in the best way possible.

d. Provide cross functional development capacity and implement software in sprint timelines as approved by the GMM Product Manager. The Contractor shall advise and provide input toward defining sprint timelines. The Contractor shall deliver fully functional epics in each quarterly increment, according to committed timeframes and scope. The implemented solution shall address existing capability gaps as defined by the MNS and GMM's requirements as documented in the ORD.

e. Maintain a source code repository in BitBucket. The Contractor shall follow industry best practices to implement continuous integration and continuous deployment. These efforts will include the management and maintenance of the AWS cloud infrastructure and the DevSecOps process working in tandem with the incumbent support personnel. The Contractor shall design, develop, and deploy software according to the development priorities established by the GMM Product Owners.

f. Migrate and/or develop functionality and business processes from legacy disaster and non-disaster grants programs into the target GMM platform.

g. Integrate the target GMM platform to all external data sources needed to support AFG, HMA, PA, Preparedness and IA grant programs, as identified by GMM Product Management and Engineering.

h. When relevant, identify and propose additional metrics for technical performance, business success, and user satisfaction.

i. Leverage current investment and existing approved technologies, streamlined business processes, data models, design, wireframes, architecture, cloud systems, technology stack, etc.

j. Engage in knowledge transition of development and business processes for all target grants management programs, while ensuring there are no negative impacts on other team's productivity.

k. Investigate emerging technologies and industry best practices relevant to FEMA GO and provide recommended solutions for FEMA to consider. Once the Government agrees on the recommendation, the Contractor shall begin to leverage emerging technologies and implement proposed solutions.

l. Provide all relevant documentation to support system managers in implementing the target solution.

VII. DELIVERABLES AND DELIVERY SCHEDULE

Deliverables and Delivery Schedule shall be determined at the call order level.

Deliverables and Delivery Schedule may include but are not limited to:

No.	Task	Deliverable	Frequency and/or Due Date	Format
1	6.1 c	Post Award Kick-Off Meeting	5 work-days (WD) after award	In person or virtually
2	6.1 d 6.1 e 6.1 f	Updates to Project Management Plan that incorporates Quality Control Plan, Change Management Plan, and Staffing Plan	Updates as needed and communicated with the COR. Updates to the PMP and operational model shall be submitted within one week of agreement, approval, or realization of the change.	Electronic
3	6.1 g 6.1 k	Monthly Status Report, which shall include root cause analysis for all performance metrics that were not met and # of deployments	Monthly, by the 10th business day of the month	Electronic
4	6.1m 6.1n 6.2 h	Delivery status updates of metrics and updates to Dashboard	Weekly/As Scheduled, date to be communicated by the COR	Electronic
5	6.2 g	Conduct Integration Test and Evaluation (IT&E) for Agile Development Releases	Per Product Roadmap	Electronic
6	6.2 a	Delivery of software functionality	Constant as defined by the quarterly Product Roadmap Program Increment. Deliver software functionality	Electronic

			according to Roadmap Planning and Dev Done Planned dates, factoring in sufficient time for IV&V and UAT timelines.	

VIII. QUALITY CONTROL:

The Contractor shall provide a QCP at the BPA level and at the call order level. The QCP shall identify the Offeror's approach for maintaining a quality control system that is integrated into the overall project management plan and meets requirements of the PWS. The Contractor's QCP shall address the associated metrics. The Contractor's QCP shall be linked to the PWS' Performance Requirements Summary (PRS). The Contractor shall be solely responsible for the quality of services provided. The Contractor shall also be liable for Contractor employee negligence and any fraud, waste or abuse.

The Government shall provide a copy of its draft QASP to the Contractor as part of the solicitation documents. Following approval of the Contractor's QCP and making award, if the Government determines that updates to its QASP are necessary based on the approved QCP, the Government shall provide an updated copy of its QASP to the Contractor within 30 days of the award. If the Government determines that no updates or changes to the QASP are necessary at that time, the Government shall inform the Contractor.

The Contractor shall maintain the QPC throughout the life of the contract. The QPC shall outline the processes and activities the Contractor will implement to ensure that all services are provided in accordance with the goals and requirements of this PWS. QC is work output, not workers, and therefore includes all work performed under this contract regardless of whether the work is performed by Contractor employees or by subcontractors. The Contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The QCP shall fulfill the following requirements:

i. Establish an internal quality control, inspection and feedback system for all services required by the contract.

ii. Provide the means to identify deficiencies in services and procedures to correct deficiencies and prevent recurrence.

The QCP shall include, but not be limited to, the following elements:

i. Methods to track timeliness and performance with respect to established standards for responsiveness and quality of service.

ii. Methods to measure the effectiveness of the Contractor's quality control actions.

iii. The QCP will also identify the individuals within the Contractor's organization with oversight authority over quality initiatives.

The Contractor's QCP shall address how to handle Inspection and Acceptance Criteria, Delivery and Timing, the Collaboration Environment, any Service Level Agreements, the draft Quality Assurance Surveillance Plan (QASP), and Quality Controls related to, but not limited to:

i. Contract Deliverables
ii. Cybersecurity Corrections
iii. Audit/Evaluation Corrections
iv. Corrective Actions Plans and Validations
v. Software Defects or Issues, Priority of Critical/Moderate/Low
vi. Error Detection in Production, Rate and Count
vii. Deployment to Production, Failed vs First Time Success
viii. Attrition and Recruiting
ix. Team Velocity and burn down
x. Availability and Website Uptime
xi. U.S. Web Design Standards / 21st Century Integrated Digital Experience Act (P.L. 115-336§3(e))

These should also include the Definition, Acceptable Quality Level / Performance Standard, Actual Measurement, Reporting Frequency, Method of Surveillance, etc.

IX. PERFORMANCE REQUIREMENTS SUMMARY

In accomplishing the performance objectives of this PWS, the contractor shall be responsible for achieving and maintaining the performance standards outlined in the Performance Requirements Summary (PRS).

The table below specifies performance metrics with corresponding performance standards, surveillance methods, and incentives. These metrics apply to all work performed within each of the work areas. The COR and Task Manager of this contract will document high quality performance and ensure it becomes part of the Contractor's past performance record, which will be entered at least annually into the Contractor Performance Assessment Reporting System (CPARS).

Incentive: COR will document high quality/high performance and ensure it becomes part of Contractor's past performance record which will be entered at least annually into CPARS.

Disincentive: COR will document low quality/poor performance and ensure it becomes part of Contractor's past performance record which will be entered at least annually into CPARS.

Performance Requirements may be established at the call order level. Performance metrics may include but are not limited to:

Category (Task)	*Required Services / Desired Output*	*Performance Standard / Threshold*	*Monitoring Method*
Cybersecurity	Remediation of vulnerabilities identified in ST&E or Security Operations Center (SOC) mandated scans (Critical/High/Medium/Low)	Critical - # of days High – # of days Medium – # of days Low – # of days	Security scan reports (As Required)
Invoices	Submission of timely and accurate invoices	Accurate and complete invoice reports each month	COR monitors and reviews invoices (Monthly)
Meetings	Organized and productive meeting facilitation	% of meetings facilitated by the Contractor that are properly coordinated. Planning incorporates necessary meeting materials to include an agenda articulating a purpose and outcome(s) published in advance of the meeting. Meeting time is well managed, and the purpose and outcome(s) are achieved.	GMM Program Management Office will provide performance feedback to the COR and/or CO regarding meeting experience. (As scheduled)
Quality of Written Deliverables and Reporting	Effective, clear, and concise writing and reporting.	% of deliverables that do not include significant mistakes or require significant rework before being accepted by the Government.	GMM Task Manager, COR, and/or CO review submitted deliverables and reporting (As received)
Timeliness of Written Deliverables	Submission of timely and complete reports and other written contract deliverables	% of complete and accurate updates to the PMP, operational model, Quality Control Plan, Change Management Plan, and Staffing Plan made within the required time from agreement, approval, or realization of the change. % of complete and	COR monitors due dates and notes when deliverables are submitted/ completed (Per Schedule of Deliverables)

		accurate Monthly Status Reports submitted on time (e.g. includes root cause analysis for all performance metrics that were not met, includes # of deployments)	
Quality - Defects	**Defect Density of Critical and Major Defects** **(Critical/Major per Million Lines of Code)**	# of Critical/ Major O&M Production Defects	Included in Monthly Report and dashboard (Monthly and ad hoc)
	Defect Detection per Phase	Critical/Major Production – # detected UAT – # detected IV&V – # detected Development – # detected Moderate/Minor/Minimal Production – # detected UAT – # detected IV&V – # detected Development – # detected	Included in Monthly Report and dashboard (Monthly and ad hoc)
Reporting of Technical efficiency and velocity	Timely reporting of progress made per sprint	Timely reporting of progress made per sprint	Included in Monthly Report (Monthly)
Business Value / Schedule	Achieving committed outcomes within each Product Increment; delivery of deployable functionality	% of committed outcomes within each increment	Monthly Status Reports (Monthly and Per Product Increment)
Outcome Schedule Variance	Variance / Estimate	-%/+% of committed outcomes vs actuals for an increment	Monthly Status Reports (Monthly and Per Product Increment)
Increment Schedule Variance	Sum of Variance for All Outcomes / Sum of Estimates for All Outcomes	-%/+% of committed outcomes vs actuals for an increment	Monthly Status Reports (Monthly and Per Product Increment)
Accessibility	Accessibility of FEMA GO for compliance under Section 508	Compliance	IV&V Accessibility Test Report (Weekly)
Code Quality Regression Testing	Regression Testing of Submitted Code	% of submitted code that passes regression testing	Regression Testing (Per Phase / Per Release)

Availability	FEMA GO is available with no down time during deployments	% of availability	New Relic / AWS CloudWatch logs (ad hoc / spot testing)

X. Key Personnel

The Contractor shall identify key personnel and provide statements of qualifications for these individuals. In accordance with the BPA and each call order, the Contractor shall provide any Key Personnel determined at the call order level. Key Personnel shall sign a non-disclosure agreement. Key personnel will not perform work at the BPA level. All work will be performed at the call order level.

Key Personnel may include but are not limited to:

- **Management lead (minimum of 12 years of relevant experience)** - The management lead shall ensure that all work complies with terms and conditions and shall have access to contractor corporate senior leadership when necessary. The Contractor's management lead shall be the primary interface with the FEMA Contracting Officer's Representative (COR) and Contracting Officer (CO) and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by the technical lead when necessary. Management lead should have a minimum of 12 years of relevant experience. Depth and quality of experience, education, and training relevant to the responsibilities of the position.
- **Technical lead (minimum of 12 years of relevant experience)** – The technical lead shall ensure the solutions delivered meet FEMA's functional and non-functional requirements.
- **Product Management lead (minimum of 12 years of relevant experience)** – The product management lead shall ensure product management activities comply with the Federally governed delivery approach and incorporate industry best practices.
- **Test and Evaluation lead (minimum of 12 years of relevant experience)** – The test and evaluation lead shall ensure the solutions delivered meet or exceed FEMA's quality requirements.
- **User Research lead (minimum of 8 years of relevant experience)** – The user research lead shall ensure user research and design activities comply with the Federally governed delivery approach and incorporate industry best practices.
- **Business Analysis lead (minimum of 8 years of relevant experience)** – The business analysis lead shall ensure discovery, requirements elicitation, and documentation activities comply with the Federally governed delivery approach and incorporate industry best practices.

Qualifications of Key Personnel shall be considered based on the depth and quality of experience, education, and training relevant to the responsibilities of the position(s). Experience that is closer to the scope of the requirement is preferred.

FEMA will review the statements of qualifications provided for Key Personnel to ensure they meet the contractual requirements for performance and provide confirmation of such assessment in writing from the Contracting Officer (CO). If the performance of Key Personnel does not meet or exceed the expected performance of an individual with the supplied statement of qualifications, the Government will request, and the Contractor will submit a FEMA approved replacement for fitness/security screening to FEMA security within 30 days. Any such request will be made at the discretion of the Government, and in writing by the Contracting Officer (CO).

The Contractor shall not replace any Key Personnel without prior approval by the Government. The Contractor shall provide any request to replace any Key Personnel in writing to the Contracting Officer (CO) and Contracting Officer's Representative (COR) no less than two weeks (10 business days) prior to the departure of the Key Personnel. The request shall indicate the proposed transition period and identify the replacement Key Personnel including a summary of qualifications. The Government will provide written approval or disapproval from the Contracting Officer within one week (5 business days) of receipt of the request. If the request is disapproved, the Contracting Officer shall indicate in writing the reason for disapproval. The Contractor shall not be bound by this requirement if the Key Personnel is terminated for cause, resigns, or is medically incapacitated. If the Key Personnel is terminated for cause resigns, or is medically incapacitated, the Contractor shall submit a FEMA approved replacement for fitness/security screening to FEMA security within 30 days. Documentation of these exceptions shall be provided to the Government. All proposed replacements shall possess qualifications equal to or superior to those of the Key Personnel being replaced, unless otherwise approved by the Contracting Officer.

XI. Associate Contractor Agreements and Communications Plans

The Contractor shall enter into written agreements with other FEMA contract holders hereinafter called "associate contractors," within 60 days of Government notification, to facilitate effective joint collaboration necessary to perform work under this requirement. Associate contractors will be identified in specific contracts. Accordingly:

a. The Contractor shall execute written agreements with individuals and organizations identified by the Government as associate contractors. The agreements shall provide for effective communication between counterparts at all levels from senior corporate management to working engineers. The agreements shall include the condition that any proprietary information furnished by an associate contractor pursuant to the work under this contract will be protected from unauthorized release or disclosure beyond the scope of the agreements. Further, the agreements shall hold the Government harmless from liability for the unauthorized disclosure by the Contractor of associate contractor proprietary information.

b. The Contractor shall freely and directly exchange information on the performance of its efforts. The Government may conduct meetings to facilitate the exchange of information and data between and among associate contractors and other Government personnel. The Contractor shall participate in such meetings. In the event of a disagreement as to what constitutes a

permissible exchange of information or data under agreements, the Contracting Officer will have final decision authority.

XII. Travel

Travel is not anticipated to be part of the work, and travel expenses subject to cost reimbursement are not anticipated. Otherwise, any travel would be at the call order level.

XIII. Additional Contract or Personnel Requirements

A. Kick-Off Meeting

The Contractor shall conduct a kick-off meeting within 5 calendar days of contract award. The Contractor shall provide briefing slides at the kick-off meeting that include information on the approach to each task, all events and milestones, staffing and program status. The Contractor's project management and key personnel staff should attend the kick-off meeting. The kick-off meeting shall be conducted at FEMA facilities or virtually, as agreed upon.

B. Monthly Report and Status Meetings

The Contractor shall submit a monthly report for the work performed during the period. To include (but not limited to) the following sections and suggested breakouts:

- Contract Information: such as: Contract number, order Number, Award Information, Date of Award, CO's (Government and Contractor), COR, requisition number, etc.
- Executive Summary of Tasks Accomplished during Reporting Period: Section 4.0 Task section of the PWS.

C. Monthly Status Meetings

The Contractor shall actively participate in monthly status meetings with the COR, GMM Task Manager, other identified members of the GMM Program, Contractor PM, and other representatives, as appropriate, to discuss status of the contract and associated deliverables as well as identify risks and propose mitigation strategies.

XIV. Invoice Requirements

a. Period of Invoices

Monthly invoices shall be submitted for all costs accrued during the monthly reporting period. The monthly reporting period may be a calendar month, or any other period used by the Contractor as a billing cycle, providing that this billing cycle has no fewer than 28 days and no more than 31 days in it.

b. Invoice Submission Method

The Government prefers electronic copy of the invoice and backup documentation submitted to FEMA-Finance at the email below as well as to the designated COR and CO the following:

1. FEMA Invoices: FEMA-Finance-Vendor-Payments@fema.dhs.gov

c. Timeliness

Invoices shall be submitted within three (3) working days of the end of each calendar month or the Contractor's accounting cycle.

XV. SECTION 508 REQUIREMENTS:

Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

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

Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

4. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.

5. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

6. When developing or modifying software functions of ICT, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including the requirements in Chapter 5 and WCAG 2.0 Level A and AA Success Criteria). When the requirements in Chapter 5 do not address one or more software functions, the Contractor shall demonstrate conformance to the Functional Performance Criteria specified in

Chapter 3. The Contractor shall use a test process capable of validating conformance to all applicable Section 508 standards for software functionality delivered pursuant to this contract. The Contractor may utilize the DHS Trusted Tester Methodology for Web and Software Version 4.0 as a component of the overall test process used. This version of the test process provides partial test coverage of the Section 508 standards that apply to software. If the Contractor uses this test process, the Contractor shall address the test coverage gaps through additional test procedures. Information on the DHS Trusted Tester Methodology for Web and Software Version 4.0, including coverage against the applicable Section 508 standards for software as well as gaps that need to be addressed through other test methods, related test tools, and training is published at https://www.dhs.gov/trusted-tester.

7. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the 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 project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

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 developed or modified pursuant to this contract), the Offeror 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.

4. **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:

    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.

- Documentation of remediation plans to address non-conformance to the Section 508 standards

XVI. DHS ENTERPRISE ARCHITECTURE COMPLIANCE:

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

(a) All developed solutions and requirements shall be compliant with the HLS/FEMA EA.

(b) All IT hardware and/or software shall be compliant with the HLS/FEMA EA Technical Reference Model (TRM) Standards and Products Profile.

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

(d) Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01[1] and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

(e) Applicability of IPv6 to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

XVII. 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.

[1] Department of Homeland Security (DHS) Directives System, *Enterprise Data Management Policy*, 2008. https://www.dhs.gov/sites/default/files/publications/mgmt_directive_103_01_enterprise_data_management_policy.pdf

The term Federal record:

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

C. *Requirements*

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

facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the PWS. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-Contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-Contractor) is required to abide by Government and FEMA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with FEMA policy.
8. The Contractor shall not create or maintain any records containing any non-public FEMA information that are not specifically tied to or authorized by the contract.
9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.
10. The FEMA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which FEMA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take FEMA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

XVIII. SECURITY REQUIREMENTS:

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

- FAR 52.224-3 Privacy Training – Alternate I
- HSAR 3052.204-71 Contractor Employee Access
- HSAR 3052.204-71 Contractor Employee Access Alt I
- HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information

- HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information Alt I
- HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents
- Information Technology Security Awareness Training
- FAR 52.204-9 Personal Identity of Contractor Personnel

BACKGROUND INVESTIGATIONS:

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

Low Risk without Information System Access
Contractor personnel occupying positions or performing functions with a low risk designation and who do not require access to DHS or FEMA information systems shall undergo a Tier 1 (T1) background investigation which is equivalent to the previously identified National Agency Check with Inquiries (NACI). Either of these investigations must be supported by a separate credit check and must receive a favorable adjudication thereof from FEMA PSD prior to holder performing work under this contract. A favorably adjudicated NACI & C will remain acceptable for the purpose of reciprocity where a T1 investigation is required for a period of 5 years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

Low Risk with Information System Access
Contractor personnel occupying positions or performing functions with a moderate risk designation shall undergo a Tier 2 Suitability (T2S) background investigation which is equivalent to the previously identified Moderate Risk Background Investigation (MBI), and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated MBI will remain acceptable for the purpose of reciprocity where a T2S investigation is required for a period of 5 years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

Moderate Risk
Contractor personnel occupying positions or performing functions with a moderate risk designation shall undergo a Tier 2 Suitability (T2S) background investigation which is equivalent to the previously identified Moderate Risk Background Investigation (MBI), and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated MBI will remain acceptable for the purpose of reciprocity where a T2S investigation is required for a period of 5 years from the date of

completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

High Risk
Contractor personnel occupying positions or performing functions with a high risk designation shall undergo a Tier 4 (T4) background investigation which is equivalent to the previously identified Background Investigation (BI), and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated BI will remain acceptable for the purpose of reciprocity where a T4 investigation is required for a period of 5 years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

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

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

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

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

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

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

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

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

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

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

Once Contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant Contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the Contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified Contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the Contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the 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 T1, T2S, or T4 (or the equivalent OPM investigation) are valid for five years from the date that the investigation was completed and closed. Contractor personnel required to undergo a background investigation to perform work under this contract shall be ineligible to perform work under this contract upon the expiration the background investigation unless and until the Contractor personnel have undergone a reinvestigation and FEMA's Personnel Security Division has renewed their eligibility to perform work under this contract.

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

FACILITY ACCESS:

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

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

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

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

SEPARATION FROM CONTRACT:

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

- When no longer needed for contract performance.

- Upon completion of a Contractor employee's employment.
- Upon contract completion or termination.

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

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

FOR OFFICIAL USE ONLY:

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

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

Contractors and Consultants shall:

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

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) [https://securityawareness.usalearning.gov/disclosure/index.html]

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)
[https://securityawareness.usalearning.gov/opsec/index.htm]

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

INSIDER THREAT TRAINING:

Insider Threat training for Contractors can be found at: Insider Threat Awareness (usalearning.gov) [https://securityawareness.usalearning.gov/itawareness/index.htm]

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

FOREIGN TRAVEL AND GOVERNMENT-ISSUED EQUIPMENT

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

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

FedRAMP Certified Language

- **The proposed cloud solution must be FedRAMP certified. Reference:** Federal Risk and Authorization Management Program (FedRAMP), http://www.fedramp.gov:
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce (DOC), Special Publication (SP) 500-292, *NIST Cloud Computing Reference Architecture*, September 2011.
- NIST, U.S. DOC, SP 800-145, *NIST Definition of Cloud Computing*, September 2011.

HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) *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, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All

Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the contractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

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

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right,

a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

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

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

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

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

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

(End of clause)

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

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

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

(1) Chemical-terrorism Vulnerability
Information (CVI) as defined in 6 CFR part 27, ''Chemical Facility Anti-Terrorism Standards,'' and as further described in supplementary guidance issued by an authorized

official of the Department of Homeland Security (including the Revised Procedural Manual ‘‘Safeguarding
Information Designated as Chemical-Terrorism Vulnerability Information’’ dated September 2008);

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

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, ‘‘Protection of Sensitive Security Information,’’ as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, ‘‘Sensitive Security Information (SSI)’’ and, within the Transportation Security Administration, TSA MD 2810.1, ‘‘SSI Program’’;

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

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

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

> (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples

of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

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

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

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

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

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

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

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.
Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

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

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

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

(b) Handling of Controlled Unclassified Information.

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

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

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

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

(c) Incident Reporting Requirements.

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https:// www.dhs.gov/dhs-security-and-trainingrequirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier

subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

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

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

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

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);

(v) Contracting Officer POC (address, telephone, and email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.
(d) Incident Response Requirements.

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

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

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

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate
(ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

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

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information. Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it
physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to

the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, Guidelines for Media Sanitization, Appendix G.

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

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

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

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023), or any successor publication; and the Security Authorization Process Guide, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-trainingrequirements- contractors.

(i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and

Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the
SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

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

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

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

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

all requested images),for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

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

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023), or any successor publication; and the Security Authorization Process Guide, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate

(4) Federal Reporting and Continuous Monitoring Requirements. Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information

Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhssecurity-and-training-requirements contractors.
The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(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 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, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized 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)

FAR 52.224-3 Privacy Training (Jan 2017)

(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 24.3 and 39.105).

(c)(1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-

(i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

(ii) The appropriate handling and safeguarding of personally identifiable information;

(iii) The authorized and official use of a system of records or any other personally identifiable information;

(iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information;

(v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

(vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.

(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)

Alternate I (Jan 2017). As prescribed in 24.302 (b), if the agency specifies that only its agency-provided training is acceptable, substitute the following paragraph (c) for paragraph (c) of the basic clause:

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

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

(b) *Security Training Requirements*.

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

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

XIX. PRIVACY REQUIREMENTS RESPONSIBILITIES

To accomplish the tasks outlined in this contract, FEMA will provide the contractor access to the Grants Technology Division - Streamlined Platform for Agile Release and Transformation Acceleration (SPARTA) and all the PII/SPII that is contained within the system.

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

DHS/FEMA/PIA-052 Grants Management Modernization (GMM).

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

DHS/FEMA-004 Non-Disaster Grant Management Information Files; Routine Use H
DHS/FEMA-008 Disaster Recovery Assistance Files; Routine Use F
DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs; Routine use F
DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), Routine Use F
DHS/ALL-026 DHS Personal Identity Verification Management System Routine Use F

To accomplish the tasks outlined in this contract, the contractors will have access to PII of first name, last name, email addresses, FEMA employees via Global Address List (GAL) by way of FEMA laptops use. The information sharing is authorized by Routine Use F of DHS/ALL-014 Department of Homeland Security Personnel Contact Information "March 16, 2018, 83 FR 11780. The information sharing is also covered by the following Privacy Impact Assessments:
DHS/FEMA/PIA-052 Grants Management Modernization (GMM).

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

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

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

Authorities
This information sharing outlined in this contract is authorized by The Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. §§ 5121-5206 (2013); Debt Collection Improvement Act of 1996 (31 U.S.C. § 7701(c)(2)); the Homeland Security Act of 2002, Pub. L. No. 107-296, Title V (2002) (codified as amended at 6 U.S.C. §§ 311-321n); the Privacy Act of 1974 as amended (2012), 5 U.S.C. § 552a et seq. (Privacy Act).

FedRamp Certified language

- **The proposed cloud solution must be FedRAMP certified. Reference:** Federal Risk and Authorization Management Program (FedRAMP), http://www.fedramp.gov:
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce (DOC), Special Publication (SP) 500-292, *NIST Cloud Computing Reference Architecture*, September 2011.
- NIST, U.S. DOC, SP 800-145, *NIST Definition of Cloud Computing*, September 2011.

(a) Cloud computing. All use of cloud computing products or services that process unclassified information must comply with the FedRAMP Authorization Act, 44 U.S.C. Section 3607 et. seq. The following requirements apply when using cloud computing to provide information systems or services in the performance of the contract.

i. Cloud computing security requirements. The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with FedRAMP Security Authorization Requirements unless notified by the Contracting Officer that this requirement has been waived by the Agency Chief Information Officer.

ii. Cloud computing continuous monitoring. The Contractor shall maintain an adequate continuous monitoring capability based on the FedRAMP Security

Authorization Requirements including processes described in the NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and governed by the FedRAMP Continuous Monitoring Strategy Guide.

iii. Cloud computing services cyber incident reporting. The Contractor shall report all cybersecurity incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted according to FedRAMP Security Authorization Requirements, published FedRAMP Incident Communications Procedures, and Federal Incident Notification Guidelines for submitting incident notifications to CISA using the CISA incident reporting form (https://us-cert.cisa.gov/report).

Artificial Intelligence Clause

The Contractor will not use or deploy the use of Artificial Intelligence, as defined by 15 U.S.C. 9401(3), unless expressly authorized by the Contracting Officer.

The term ‘‘artificial intelligence’’ means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to –
(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action.

DHS Geospatial Information System Compliance

All implementations that require access to the DHS Geospatial Information Infrastructure (GII), including geospatial data, information, and services shall comply with the applicable policies and requirements set forth in the GII, including (but not limited to) the following:

• All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.

• All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

OCIO CISO Cyber-Supply Chain Risk Management (C-SCRM) SOW Language 6.29.2023

a. Definitions

i. 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.

ii. 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).

iii. 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).

iv. 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).

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

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

i. 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.

ii. 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.

c. Accounting of Components in ICT Products

i. 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.

ii. 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.

iii. 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.

iv. 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.

d. Supply-Chain Transport

i. 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.

ii. 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.

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

iv. 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.

v. 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.

e. Changes to Ownership and Control

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.

XX. Acronyms (for Sections I through XII)

AFG	Assistance to Firefighters Grants

ALF	Acquisition Lifecycle Framework
AoA	Analysis of Alternatives
ATO	Authority to Operate
CO	Contracting Officer
CONOPs	Concept of Operations
COR	Contracting Officer's Representative
DHS	Department of Homeland Security
DPW	Development Pair Week
EA	Enterprise Architecture
FEMA	Federal Emergency Management Agency
FEMA GO	FEMA Grants Outcomes
FFP	Firm Fixed Price
FOC	Full Operational Capability
GMM	Grants Management Modernization
HMA	Hazard Mitigation Assistance
IA	Individual Assistance
ILSP	Integrated Logistic Support Plan
IPR	In Progress Review
IT	Information Technology
MNS	Mission Needs Statement
O&M	Operations and Maintenance
ORD	Operational Requirements Document
PA	Personal Assistance
PMP	Project Management Plan
POC	Point of Contact
POP	Period of Performance
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
SELC	Systems Engineering Lifecycle
SOC	Security Operations Center
TEMP	Test and Evaluation Master Plan

Rest of This Page Intentionally Left Blank