DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
CYBERSECURITY AND INFRASTRUCTURE SECURITY
INFRASTRUCTURE SECURITY DIVISION
SECTOR RISK MANAGEMENT AGENCY (SRMA) NATIONAL PLAN IMPLEMENTATION, DATA, INFORMATION SHARING AND STRATEGIC SUPPORT

August 2022

1. Unclassified (U) GENERAL

1.1 (U) BACKGROUND

The CISA Act of 2018 created the Cybersecurity and Infrastructure Security Agency (CISA) as an operational component within the Department of Homeland Security (DHS).

As an agency, CISA is tasked with securing the Nation's cyber and physical critical infrastructure. There are currently 16 critical infrastructure sectors that have been identified in PPD-21 which spells out the policy for how the federal government builds trusted partnerships and "advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."

Within CISA, the Infrastructure Security Division (ISD) is the lead organization responsible for implementing and coordinating national programs and policies on critical infrastructure security and resilience, and manages the National Infrastructure Protection Plan (, last updated in 2013) required pursuant to 6 USC 652(e)(1)(E). Pursuant to statutory authority, ISD conducts and facilitates vulnerability and consequence assessments to identify the nation's critical infrastructure, understand how it is vulnerable, and take action to reduce risks to it. ISD also works with critical infrastructure owners and operators, and State, local, tribal, and territorial partners understand, prioritize, and address risks to critical infrastructure. ISD also provides information on emerging threats and hazards so that appropriate actions can be taken, and it offers tools and training to partners to help them manage the risks to their facilities and operations. This office has established strong partnerships across government, the private sector and actively collaborates with the SRMAs from across all Critical Infrastructure sectors. It is imperative that the ISD has the proper resources, support, and capabilities in order to continue to expand upon the vital services that the division offers relating to critical infrastructure security.

As director of one of three statutory CISA Divisions, the Executive Assistant Director of the Infrastructure Security Division is authorized to direct the critical infrastructure security efforts of the Agency on behalf of the Director. The Strategy, Performance, and Resources (SPR) team is responsible for enabling the Assistant Director's responsibility by supporting ISD core functions through division level strategy, strategic plans, and issuing Agency operational guidance. SPR is also responsible for maintaining

National infrastructure security and resilience doctrine including the National Infrastructure Protection Plan (now known as the National Plan). Sector Risk Management Agencies (SRMAs) have been at the forefront of sector infrastructure security initiatives and serve as the day-to-day Federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific activities. These agencies are also tasked to carry out incident management responsibilities and provide support and other technical assistance to help identify and mitigate vulnerabilities and incidents.

Strategic doctrine and the collaboration that has augmented its implementation has significantly expanded the ISD's ability and need to provide services to our FSLTT partners and further partnerships in better protecting Critical Infrastructure. Additional general support will be needed involving initiatives like the National Plan and its socialization, implementation, and periodic refresh; Strategic Policy and Planning initiatives; and other data and information sharing support that operationalize the goals and objectives found in the National Plan and other related laws and doctrine.

This contract support will provide technical and mission support services to ISD Strategy, Performance, & Resources (SPR) with the goal of enhancing and expanding upon implementation of the goals and objectives under the National Plan [required pursuant to 6 USC 652(e)(1)(E)], current data, information sharing, and strategic services that are being provided to SRMAs and other FSLTT stakeholders as they complete their operational responsibilities.

The 2022 National Plan describes how stakeholders collaborate to build an all-encompassing understanding of critical infrastructure risk. The National Partnership Structure enables stakeholders to work together to identify risks and vulnerabilities, secure critical systems and assets against direct threats, and build resiliency by providing standards and tools to help the critical infrastructure community adapt to industry standards. The expanded scope of the plan has led to a capability gap in resources available to help further execute on the plan's goals. Specifically involving the further maturation of National Plan supplements, subsequent plan updates, FSLTT socialization methods, and technical expertise involving the collection, aggregation, analysis, and dissemination of relevant information/intelligence and data to and from our private and public sector partners.

To fulfill this mission, ISD requires contractor support to assist in activities related to program development, operational support, communications, training, technical assistance, and other administrative and analysis functions beginning in 2022 for up to 5 years. This task benefits ISD as we move forward with further developing our internal capabilities, processes, and procedures in support of internal and external stakeholders.

Additionally, SPR is charged with capability development to support execution of these strategy. ISD's mission relies on our ability to collect, manage, interpret, and disseminate data. Data, analysis, research, and technology are vital avenues through which ISD develops the capabilities required to meet Division statutory responsibilities, and strategic goals and objectives. This includes the frameworks, tools, data, research, and technology that enable ISD to meet its mission. There are a wide range of agency resources and initiatives for accessing outside support in these areas—including:

- Vulnerability Assessments conducted through the Regions (IOD)Protected Information collected and managed through the National Plan partnership and through ISD assessment tools.
- The National Infrastructure Simulation and Analysis Center (NISAC), administered through the National Risk Management Center (NRMC)
- CISA Chief Technology Officer strategic priorities
- Interagency Agreements established across the Department and within CISA for accessing FFRDCs

CISA's authorizing legislation includes a requirement for the Agency to integrate information, analysis, and vulnerability assessments—including assessments carried out by other Federal Agencies, or industry partners. This integration function is also explicitly tied to ISD's capacity building mission, and drives our ability to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

1.2 (U) OBJECTIVE/SCOPE

Under this contract, the contractor shall provide technical and general mission support services to ISD SPR office elements located in the National Capital Region (NCR).

The Contractor shall demonstrate through a staffing plan and resumes that it will provide trained and qualified personnel with appropriate education and/or experience in critical infrastructure and executive level to perform the program management and specialized technical and analytical and training support requirements in this SOW in support of ISD's mission.

The contractor shall provide support in the following areas:

I. National Plan Implementation Support

II. Data and Information Sharing Program Management Office (PMO) Support

III. Strategic Policy and Planning Support

The contractor will be expected to lead efforts by ISD to integrate and implement future critical infrastructure prioritization initiatives, which include providing regular updates to the Infrastructure Data Taxonomy, developing an annual data collection process for SLTT/SRMA/Industry partners, updating the National Asset Database (NADB) yearly, preparing the NADB report per 6 USC 664 requirements, and providing analysis of data that is collected.

1.3 (U) STRATEGIC INTENT, MISSION, AND VISION

The Cybersecurity and Infrastructure Security Agency (CISA) Strategic Intent (August 2019) states: "CISA's purpose is to mobilize a collective defense of our nation's critical infrastructure. This is done by

bringing together diverse stakeholders to collaboratively identify risks, prioritize them, develop solutions, and drive those solutions to ensure the stability of our national critical functions."

The ISD Mission and Vision are to secure critical infrastructure and protect lives, and to be the leader for expertise, advice, and services to secure the nation's critical infrastructure, respectively.

1.4 (U) COMPLIANCE DOCUMENTS

The Contractor shall comply with the following documents (specifications, standards, or guidelines) when executing the requirements of this SOW:

- Homeland Security Act of 2002
- Implementing recommendations of the 9/11 Commission Act
- Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Protection
- Presidential Policy Directive 8 (PPD-8): National Preparedness
- Homeland Security Presidential Directive 19 (HSPD-19): Combating Terrorist Use of Explosives in the United States
- Presidential Policy Directive 17 (PPD-17): Countering Improvised Explosive Devices
- Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience
- Executive Order 13010, Critical Infrastructure Protection
- Executive Order 13231, Critical Infrastructure Protection in the Information Age
- Executive Order 13636, Improving Critical Instructure Cybersecurity
- Executive Order 13650, Improving Chemical Facility Safety and Security
- Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- National Infrastructure Protection Plan (NIPP), 6 USC 652
- National Asset Database, 6 USC 664
- CISA Strategic Intent (August 2019)
- CISA Memorandum for Distribution: Implementation of Cybersecurity and Infrastructure Security Agency's Operating Model (January 2021)
- Statutory and Constitutional Authority of the Executive Assistant Director for Cybersecurity and the Executive Assistant Director for Infrastructure Security (January 2021; FOUO – provided post award)
- CISA Directive: Enterprise Data Management Program (September 2020)

- Sector Risk Management Agencies, 6 USC 665(d)

1.4.1 (U//FOR OFFICIAL USE ONLY (FOUO)) OTHER REFERENCE DOCUMENTS

In addition to the above Compliance Documents, the following documents may be helpful to the Contractor in performing the work described in this SOW:

- 2022 National Infrastructure Protection Plan (National Plan) Update
- National Infrastructure Protection Plan (NIPP) 2013; Partnering for Critical Infrastructure Security and Resilience
- CISA Services Catalog, Autumn 2020
- CISA Data Strategy (June 2020)
- CISA Data Governance Framework (provided post award)
- CISA Enterprise Data Models (Cybersecurity / Infrastructure Security; provided post award)
- CISA Data Governance Instruction (December 2020; provided post award)
- FY 2021 National Defense Authorization Act Section 9002(b) Report

2. (U//FOUO) SPECIFIC REQUIREMENTS and TASKS

(U//FOUO) For all tasks, the contractor, via the contract Program Manager, shall manage the work that is assigned under sections 2.1 through 2.5. All contractor personnel shall be able to read, write, speak, and understand English.

Requirements identified below are required for the contractor to successfully perform the tasks identified in 2.1 through 2.5. These are:

a. Leverage the full suite of Microsoft Office 365 (to include PowerPoint, Visio, Project, OneNote, SharePoint, PowerBI) for task management, execution, delivery, and knowledge management.
b. Perform work on the DHS Unclassified (A-LAN), Secret (HSDN) and Top Secret/SCI (C-LAN) networks as appropriate and maintain their user accounts on all applicable networks.
c. Assist in the preparation of documentation, correspondence, briefing materials, and other related documentation in support of day-to-day operations.

2.1 Task One. Program Management

In order to help our FSLTT partners successfully implement the National Plan's goals and objectives at an operational level, it is imperative that ISD SPR has the capability to conduct performance management, track productivity, and understand the effectiveness of National Plan Implementation initiatives.

Contractors shall anticipate developing and delivering unclassified or classified products up to TS/SCI. All Key Personnel are expected to have active, in-scope Top Secret clearances and eligibility for SCI access. The contractor shall also have access to backup and surge staff capable of supporting at the TS/SCI level. All other staff need only have unclassified DHS fitness/suitability.

2.1.1 Task Order Management

Program management and project control are inherent to each task area under the task order. The Contractor shall determine the project organization and overall management to accomplish the work, how the technical management will be performed, how personnel and physical resources will be managed, and what mechanisms will be used for cost and schedule control. The Contractor shall provide the planning, direction, coordination, and control necessary to accomplish all SOW requirements.

The Contractor shall submit a Project Management Plan (PMP) describing the technical approach, organizational resources, and management controls to be employed to meet the cost, performance, and schedule requirements throughout the execution of each program task area described below. The PMP shall include productivity and management methods such as quality assurance, methods for detailed progress/status reporting and program reviews and shall indicate the provision of centralized administration and clerical, documentation, and related functions, and shall be updated as needed but no less frequently than quarterly.

The Contractor and the Government Project Managers for each of the task areas below shall hold an initial Technical Interchange Meeting (TIM) within 15 calendar days after the task order is awarded for the purpose of reviewing the requirements and establishing firm dates for the Contract Deliverable Requirements List.

The Contractor shall prepare and present Monthly Status Reports (MSRs), which address the progress/status of each of the tasks described below, including quality assurance information, any changes made in the (TIM), and serve as the vehicle that establishes firm dates for incremental deliverables. Within the MSRs, the Contractor shall provide the following:

- Tasks worked, hours expended on each task, labor categories, and personnel used per task.
- An overview of work completed, in progress, and planned for each task.
- Identification of problem areas with recommended remedial actions.
- Summary of resource expenditures.
- Status of all issues identified during the last review.

2.1.2 Post Award Conference/Contract Kickoff

The contractor shall attend a kickoff meeting with the Contracting Officer and the Contracting Officer's Representative (COR) within ten (10) business days of contract award unless directed otherwise by the government. The purpose of the Post Award Conference, which will be chaired by the CO, is to discuss technical and contracting objectives of this contract. The Post Award

Conference will be held at the Government's facility. The contractor shall submit the Kickoff Briefing at this meeting.

2.1.3 Staffing Plan

The contractor shall submit a staffing plan to be delivered 5 calendar days after award that addresses staffing requirements to perform the work on the contract and includes a plan for staffing multiple tasks and, at a minimum, the following information:

- Labor category descriptions/qualifications proposed;
- Percentage of personnel currently available by labor category by applicable task;
- Proposed approach for staffing multiple tasks; and,
- Corporate retention rates (%) for information technology/cybersecurity staff in the Washington DC Metropolitan area. Corporate or contract specific plans/perks for staff retention.

The contractor shall ensure that its staff and subcontractors have at a minimum 2 years of equivalent experience and/or professional certifications, accreditations, and proficiency relative to their areas of expertise. This expectation may specify documented professional work and experience commensurate with the level of effort. The contractor shall retain documentation of such records.

On-site seating may be limited due to space constraints.

The staffing plan shall be updated for each Monthly Status Report.

2.2 Task Two. National Plan Implementation

2.2.1 Stakeholder Communication & Engagement Support

The National Plan is a key strategic document that provides partners the ability to better protect critical infrastructure systems & assets. To ensure the National Plan, and the goals and objectives therein, are successfully socialized and implemented by FSLTT and private sector partners CISA ISD- SPR needs the capability to further communicate with and engage our stakeholders. In order to successfully perform this task, additional methodologies will need to be developed that involve mapping the goals and objectives in the National Plan to regional priorities while also considering specific vulnerabilities and intelligence requirements.

2.2.1.1 Communications Support

The contractor shall provide Communications support that may include but not be limited to the following:

- Coordination of communications with internal customers, management, and external customers.
- Integrate disparate streams of information from across the enterprise to develop effective communication, relationships, and products.

- In close coordination with the Assistant Director's Action Group, assist with preparation of speakers notes, speeches, talking points and other preparatory material for Division/Sub-Division officials.
- Develop, coordinate, and manage communication events that support awareness-building and Division/Sub-Division's mission(s).
- Design and develop assorted communication products, which may include "Case for Action" documents, white papers, fact sheets, presentations, electronic newsletters and articles, Web pages/Web sites, portals, electronic presentations, videotapes, and CDs.

2.2.1.2 Stakeholder Engagement and Relationship Management

The Contractor shall provide stakeholder engagement and relationship management services to enable all aspects of Division/Sub-Division strategic planning, performance management, enterprise resourcing, and initiative leadership. This shall include:

- Identifying key stakeholders and other necessary engagement points for ISD activities.
- Researching and identifying stakeholders' key issues and concerns relevant to ISD activities.
- Developing plans for engaging with and communicating with stakeholders.
- Developing communications materials to support engagement with stakeholders.
- Tracking and documenting previous and planned engagements with stakeholders.
- Providing administrative and logistics support to the Division/Sub-Division for external engagements.
- Engaging in prioritization of vulnerability assessments from stakeholders and the identification of intelligence requirements up to the TS/SCI level.
- Facilitating engagements with external stakeholders.
- Actively participating in identified working groups and providing situational awareness of the groups' activities.
- Supporting the communication of organizational priorities and activities to external partners.
- Track implementation of the goals and objectives outlined in the national plan
    - Create deliverables to identify and explain how CISA SRMAs fulfill their responsibilities pursuant to the National Plan
    - Create deliverables that track continuous improvement issues in order to support the next iteration and update of the National Plan.
- Develop templates, tools, and an overall framework for a Critical Infrastructure "Plan in a Box" effectively establishing an SLTT and Industry model for implementing or modeling the National Plan within their sphere of operation and authority.
    - Develop supporting briefing and summary materials identifying how the National Plan can be implemented within SLTT and Industry environments.

2.2.1.3 Administrative Tasking and Coordination Support for National Plan Implementation

The contractor shall provide administrative, programmatic, and advisory support involving any executive tasking relating to the National Plan, its implementation/socialization, or any other related deliverable or tasker. This support includes the following:

- Receive, triage, task, and coordinate taskers for completion. Taskers may be from various external entities (CISA leadership, Congress, other Federal Agencies), internal entities (other CISA Divisions or ISD Subdivisions), or self-generated (ISD tasking an external entity). Taskers may include requests for record, development of new materials, and/or staffing of decision memos for approval.
- Assisting in the preparation of documentation, correspondence, briefing materials, reports, and other related documentation in support of Division/Sub-Division activities.
- Support the drafting of original products and the consolidation of Subdivision submissions into an aggregated deliverable. Deliverables may include presentation slide decks, talking points, memorandum for record, cover letters, and informational reports. Provide technical writing, editing and quality assurance support for tasks directed by DHS leadership.
- Track and report status of received taskers in Daily and/or Monthly Progress Reports to include highlighting priority open actions for leadership, timelines, and milestones for completion (Task Tracker Report).
- Provide guidance on tasks and best practices for completion and obtain guidance from leadership if original guidance is unclear. Status shall be documented in the Monthly Progress Report.
- Maintain documentation and files in accordance with DHS Records Management guidelines.
- Develop and execute a wide range of strategic, programmatic, and tactical support to establish and maintain organizational tools and operations that support organization wide initiatives.
- Monitor and measure staff requirements, operations, and productivity patterns to identify opportunities for process improvement in order to maximize efficiency.

2.2.1.4 Technical Assistance for Stakeholder Outreach

Under the National Plan, ISD is responsible for coordinating annual outreach and coordination with the CISA Regions to advance overall coordination and communication efforts. To advance these efforts, the contractor shall plan, manage, oversee, and provide staffing to support an annual 'roadshow' to all 10 CISA Regional Offices. The contractor shall:

- Manage coordination and planning efforts with other CISA sub-components, including ISD, NRMC, CISA Integrated Operations Division (IOD), and all 10 Regional Offices.
- Plan and deliver all outreach assistance materials, to include a Program Fact Sheet, relevant presentations and read-aheads.
- Manage communications with Regional, SRMA, and other Sector Partners to ensure that all Partners are regularly made aware of deadlines, data structures, data submission requirements, etc.
- Respond to all incoming communications regarding National Plan data efforts within 24 hours.

2.2.2 National Plan Infrastructure Criticality and Prioritization Strategy

To further aid in the implementation of the National Plan, CISA needs to develop a strategy to harmonize various critical infrastructure prioritization programs across the Agency into one unified, harmonized approach. In order to accomplish this objective, the contractor shall:

- Review and synthesize various audit (GAO, OIG, etc.) reports on infrastructure prioritization to develop a baseline understanding on current infrastructure prioritization efforts across DHS and CISA.
- In conjunction with the ISD Data PMO (see Task 2.3), design requirements for a data call and listening sessions with relevant programs and principal personnel from all CISA sub-components and select external partners (SRMA, SCCs, States, etc.) involved in infrastructure prioritization efforts.
- Develop recommendations and a draft strategy for harmonizing infrastructure prioritization efforts across CISA.
- Design, plan, and execute a National Infrastructure Criticality Plenary Forum to discuss and draft a way forward for this effort.
- Finalize a draft shared national infrastructure criticality criteria and methodology to guide national and CISA efforts identify and prioritize critical infrastructure.
- In conjunction with the ISD Data PMO (see Task 2.3), develop requirements in support of data collection processes for sustaining and/or modifying this approach in the future, including recommendations on how to improve the Infrastructure Data Taxonomy.
- Develop a draft National Plan Criticality Annex which summarizes the prioritization criteria and methodology.

2.2.3 Training Support

To further aid in the understanding of the National Plan, its implementation, and the value it brings to our stakeholders and partners, ISD SPR is expanding the training opportunities available.

The contractor shall provide training support to ISD that may include but not be limited to the following:

- Coordinate with the Division/Sub-Division to identify training needs relating to the National Plan, including linking training to relevant CEU programs and credit systems.
- Assess instructional effectiveness and determine the impact of training on employee skills and KPIs.
- Research, develop, and test new training methods for the National Plan, including synchronous, asynchronous, virtual, and in person methods.
- Develop and deliver independent study (coordinated through the Emergency Management Institute or other suitable training provider), in person, and virtual training modules and supporting materials.
- Brief training deliverables with appropriate parties to seek feedback and additional direction
- Support standalone exercise facilitation support and National Plan focused briefs as requested by Division/Sub-Division staff.
- Plan and facilitate working sessions and other efforts to identify and coordinate actions to address exercise findings and lessons learned in after action reports.

- Provide support to ISD Governance process to include research and analysis, coordinating working groups and internal meetings in Government facilities, maintaining meeting minutes, creating and maintaining status reports, developing relevant presentation materials, coordinating and communicating various degrees of information with internal and external organizations, tracking action items, reviewing artifacts as necessary, and assist the Associate Director/Deputy Director in maintaining an efficient and timely process flow.
- Research, recommend, and provide as necessary, processes, electronic tools or other means that enhance the quality, efficiency, and productivity of the ISD operation.
  Assist with internal reviews/audits of CISA written policy and instruction.

2.3 Task Three. Data and Information Sharing Support

The CISA ISD SPR Data and Information Sharing PMO (hereafter, "Data PMO") will work to implement data and information management and sharing recommendations and guidance required for the proper implementation of the National Plan and to meet requirements of 6 USC 664.

The Data PMO will collect, catalog, and maintain standardized Critical Infrastructure and Key Resources (CI/KR) risk-related information to support critical infrastructure risk management through making data available to our homeland security partners. ISD is developing an innovative initiative that addresses many of the inadequacies and limitations exposed by earlier DHS infrastructure data and information sharing initiatives. While current ISD data and analytic platforms incorporate independent systems, tools, and/or capabilities, the end-state will integrate these components into an interoperable capability and workflow that supports and sustains data collection, management, and exchange.

The maximum level of classification required to perform this task is TS/SCI.

For all subtasks, the contractor shall possess knowledge and expertise with the following:

Concepts

- CISA Risk Architecture
- CISA National Critical Functions (NCFs)

Systems

- CISA Gateway (formerly Infrastructure Protection [IP] Gateway)
- CISA Modeling Capability Transition Environment (MCTE)

Tools

- IBM Rational System Architect
- Collibra Data Governance
- Tableau
- PowerBI
- ESRI ArcGIS

Data Types

- Protected Critical Infrastructure Information (PCII)

- Chemical-Terrorism Vulnerability Information (CVI)

In addition to the above broader tasking, the contractor shall be required to support the following enabling sub-tasks:

2.3.1 CISA ISD SPR Data PMO Support

The contractor shall provide all administrative, programmatic, and advisory support required to design and staff the Data and Information Sharing PMO, its implementation/socialization, or any other related deliverable or tasker. Additionally, the contractor will support initiatives to collaborate with individual Sector Risk Management Agencies (SRMAs), Sector Coordinating Councils (SCCs), infrastructure owners/operators and other appropriate parties to design, tailor and implement user-based protocols for developing or modifying infrastructure risk analytics as well as data and information sharing to help critical infrastructure stakeholders to identify safety/security weaknesses and vulnerabilities and implement potential risk mitigations. All initiatives under this support will comply with the criteria outlined in the National Plan.

This support includes the following:

- Receive, triage, task, and coordinate taskers for completion. Taskers may be from various external entities (CISA leadership, Congress, other Federal Agencies), internal entities (other CISA Divisions or ISD Subdivisions), or self-generated (ISD tasking an external entity). Taskers may include requests for record, development of new materials, and/or staffing of decision memos for approval.
- Assisting in the preparation of documentation, correspondence, briefing materials, reports, and other related documentation in support of Division/Sub-Division activities.
- Support the drafting of original products and the consolidation of Subdivision submissions into an aggregated deliverable. Deliverables may include presentation slide decks, talking points, memorandum for record, cover letters, and informational reports. Provide technical writing, editing and quality assurance support for tasks directed by DHS leadership.
- Track and report status of received taskers in Daily and/or Monthly Progress Reports to include highlighting priority open actions for leadership, timelines, and milestones for completion (Task Tracker Report).
- Provide guidance on tasks and best practices for completion and obtain guidance from leadership if original guidance is unclear. Status shall be documented in the Monthly Progress Report.
- Maintain documentation and files in accordance with DHS Records Management guidelines.
- Develop and execute a wide range of strategic, programmatic, and tactical support to establish and maintain organizational tools and operations that support organization wide initiatives.
- Monitor and measure staff requirements, operations, and productivity patterns to identify opportunities for process improvement in order to maximize efficiency.

2.3.2 Data PMO and National Plan Infrastructure Data Management

Infrastructure Data Management for ISD SPR includes the following projects:

2.3.2.1 Prioritization Program and Data Calls

Prioritization efforts as outlined in the National plan will prioritize the nation's CI/KR. This program will identify nationally significant, high-consequence assets and systems to enhance decision-making related to CI/KR protection. Assets and systems identified through this program include those that, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capability.

The contractor shall support all such data calls and data collection efforts and work with other parts of CISA, e.g., the National Risk Management Center (NRMC), for coordination on other infrastructure prioritization efforts (including but not limited to the National Critical Functions, the National Critical Infrastructure Protection Program, E.O. 13676 Section 9, and the Systemically Important Entities Program). These tasks shall include:

- Structuring an annual data call with all relevant entities
- Building a data model and data architecture to support all relevant critical infrastructure data elements managed by the ISD SPR Data PMO
- Recommending and implementing methods to execute and manage all data calls (e.g., specifying and managing data submission efforts for States, SRMAs, and other Sector Partners)

2.3.2.2 Infrastructure Data Taxonomy Update and Implementation

The Infrastructure Data Taxonomy was developed to ensure that DHS is able to communicate and disseminate information among other all government agencies regarding the nation's critical infrastructure. The purpose of the Infrastructure Data Taxonomy is to provide a common and consistent terminology that will effectively categorize infrastructure elements that are representative of each of the CI/KR sectors as described in the National Plan. The taxonomy is intended to define specific terms used by DHS to define all infrastructure types with a given sector.

ISD is currently in the process of working to refresh the taxonomy to reflect the updated sector context as well as additional feedback from key stakeholders regarding the taxonomy's application and implementation. Key tasks resulting from the update include, but are not limited to:

- Stakeholder engagement and elicitation including the development of a process to capture and adjudicate feedback and transition of infrastructure datasets and tools that leverage the current taxonomy to the new taxonomy.
- Development of training materials and delivery of training on the taxonomy for critical infrastructure stakeholders
- Development of supplementary materials to further define infrastructure security data holdings that complement and further inform the standardization of this data

2.3.3 National Asset Database (NADB) Coordination and Data Stewardship

The NAD is a planned requirement envisioned to be a robust data collection platform that includes an Infrastructure Data Warehouse (IDW), which is capable of processing infrastructure data from relevant sources. The NADB IDW will fuse data records and generate new, comprehensive composite infrastructure dataset(s) that contain accurate and complete infrastructure attributes and metadata information. The NAD will provide a single virtual source of infrastructure data, spatially and contextually accurate, that can be fully analyzed and disseminated quickly and efficiently in any situation. Once received, this information will provide decision-makers with key information to guide a variety of programs from disaster relief to national risk management and infrastructure protection.

NADB information will be available through application functionalities and capabilities that input, maintain, and query-associated information. The application will incorporate risk and vulnerability methodologies to help users conduct self-assessments or view the results of previously conducted analyses and evaluations. The NADB will reside on an extensible platform designed to host the data and tools that comprise the NADB, with the ability to connect, integrate and collaborate with existing and future capabilities/ systems within ISD and CISA including CISA Gateway.

The Contractor shall:

- Manage all data implementation, sharing, stewardship and update efforts for creation and maintenance of the NADB in accordance with the National Plan.
- Recommend strategies to the government to execute these efforts across multiple performers and entities, including various other contract and FFRDC performers.
- Identify a data steward support staff member for each individual or class of data assets held/ managed by CISA ISD which represent critical infrastructure security data assets. The contractor will support the data stewardship function as required by the CISA CDO Data Governance Enterprise Data Management Program.
- The contractor shall develop, implement, and maintain, the ISD Data Stewardship Framework.

2.3.4 Data and Information Collection Management

The Collection Management process is a six-phased structured approach to collecting infrastructure information to respond to Requests for Information (RFIs) and to identify data requirements of customers internal and external to ISD. These phases establish and implement a process for collecting information based on requirements, available resources, in addition to identifying sources of industry-accepted information. The goal of the Collection Management Process is to define "how" to collect data and detail the actions needed to respond to RFIs. The process consists of the following phases:

- Develop Requirements: receive, validate, accept/reject, prioritize, approve
- Develop Collection Plan: evaluate resources, develop draft collection, approval
- Task/Request Collection: execute collection, compile data inputs, process data, quality control

- Disseminate: finalize data, determine dissemination means, verify recipients, approve, disseminate, store and catalog
- Customer Evaluation: customer receives, information accepted, contact customer for feedback, complete evaluation/close RFI
- Evaluate Product and Process: review internal processes, update standing request list, discuss collection plan, update collection capabilities, close action item

2.4 Task Four. Strategic Policy and Planning Support

The Strategy team of ISD are responsible for engaging in, developing, and executing strategy, planning, and policy initiatives. These efforts include a wide array of tasks ranging from providing general administrative support to engaging with internal and external partners on the development of new policies or other National Security affiliated taskings.

Contractors shall anticipate developing, delivering, and involving themselves in unclassified and classified products up to the TS/SCI level for this task. Examples of work products include: Supplemental materials, Policies, and meetings.

2.4.1 Analysis and Policy Support

In order to expand upon National level doctrine and provide vital supplemental materials to augment its socialization and implementation, the Strategy Team must be able to effectively analyze needs/requirements, actively collaborate with our counterparts to further define and mature the need or initiative, and develop and execute strategic solutions to help further enhance these National Security initiatives. This shall include:

- Supporting the development and maintenance of policy documents for coordination/alignment, legislation, federal and department-wide strategy to enable the effective operations of the organization.
- Supporting the management of projects, including developing and implementing project plans and providing regular updates to Federal staff.
- Supporting the execution and improvement of governance structures.
- Assisting in ISD's responsibilities involving the National Plan and its subsequent statutorily mandated updates.
- Providing process elicitation, mapping, and improvement services.
- Supporting ISD initiatives to further develop national security related interests like the National Plan's related artifacts and materials that may be classified as high as TS/SCI.

2.4.1.1 Program/Project Analysis Management Support

The contractor shall provide Program/Project Analysis/Management support that may include but not be limited to the following:

- Provide performance metrics tracking and general strategic management support to Division/Sub-Division programs and projects to include implementations, migrations, and operations.
- Provide organizational, project, and performance management services necessary to enable all aspects of Division/Sub-Division strategic planning, policy development,

performance management, enterprise resourcing, and initiative leadership. Managing all project management tracking tools (i.e., Integrated Master Schedule, Integrated Master Plan, etc.).

- Manage and maintain information technology platforms and workflows (such as MS Project, JIRA or other platform the government chooses to utilize) to integrate all project artifacts and information.
- Support development, maintenance, and content of organizational communication mechanisms for information sharing purposes (i.e., portal, email, listservs, etc.).
- Support development and validation appropriate performance requirements and metrics for projects and programs aligned with ISD, CISA, and DHS high-level objectives, including metrics that meet OMB and DHS reporting requirements for the Government Performance and Results Act.
- Develop artifacts necessary to develop and track performance measures and other performance management tools.
- Manage data for performance metrics.

2.4.2 Strategy and Planning Support

ISD SPR implements key strategic initiatives through a rigorous planning process that requires thorough thought, active collaboration, proper resourcing, and attention to detail.

The contractor shall provide Planning support that may include but not be limited to the following:

- Supporting the development and maintenance of strategies, which establish linkage among planning elements such as vision, mission, goals, objectives, strategies, performance management initiatives and multi-year planning activities.
- Assisting ISD in national level policy initiatives—supporting ISD's role in drafting policy, managing working groups, and participating in National Security Council Staff and other national policy forums.
- Assisting ISD in aligning organizational investments in people, technology, and capital connected to its strategic objectives.
- Conducting analysis to assist the ISD in managing its portfolio of programs, including recommending process improvements and innovative technologies and methodologies that can be leveraged.
- Providing recommendations for improving the organization's priorities and business processes.
- Developing business improvement strategies in alignment with the ISD priorities.
- Providing advice and business planning services to support the development, analysis, integration, and implementation of program planning and assessment, as well as risk trade-off, requirements, alternatives, and feasibility studies that advance the goals and objectives of the organization.
- Developing long-range objectives and strategic plans with customers that identify internal and external strategic issues that could affect overall organizational effectiveness.
- Planning and coordinating business reviews, resource allocation, organizational structures, and financial analysis to maintain and support strategic and operational plans.

- Assisting the customer with development of plans that drive the execution of strategic development initiatives and implementation plans.
- Assess new business/technology opportunities and potential impacts to formulate recommendations and offer multiple courses of action for resolution.
- Preparing and delivering presentations, key data, and timely analysis of recent events, business trends, and other relevant information that impact ISD's priorities and operations to senior management, business unit leadership, and stakeholders.

2.5 Task Five. Surge Support

As deemed necessary and as approved by the Program Office, the contractor shall provide additional professional support services within the scope of this SOW. Surge support shall not deviate from the tasks already outlined in the SOW in Sections 2.1 – 2.5 and all subtasks. The Contractor shall seek Government approval in advance of incurring any costs associated with surge support. Government approval shall be authorized by the Contracting Officer.

Surge support may require contractor staff working more than 8 hours during a business day or, when operational conditions require, continuous staffing 24 hours a day, 7 days a week to support the mission. The Contractor shall provide knowledgeable and skilled personnel during times of surge for any task area identified within this SOW. The Government shall define the work to be performed via a project management plan, working hours, and duration of assignment. Surge shall be identified as a separate optional CLIN as identified in the task order and can be exercised at any time throughout the period of performance. Surge labor rates shall be the same as the labor rates for corresponding labor categories incorporated into this task order.

3. (U) CONTRACTOR PERSONNEL

Before replacing any individual designated as Key Personnel by the Government, the Contractor shall notify the Contracting Officer (CO) and the Contracting Officers Representative (COR) no less than 15 business days in advance. The contractor shall submit written justification for replacement and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the CO. The Contractor shall not replace Key Contractor personnel without approval from the CO. The Government may designate additional Contractor personnel as Key at the time of award or through a contract modification.

3.1 (U) QUALIFIED PERSONNEL

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

3.2 (U) PERSONNEL SECURITY

All contract personnel associated with or working on this contract, including sub-contractors, must complete DHS security, onboarding processes, and fitness determination as well as obtain a Final Entry on Duty (EOD) decision before doing any work for this contract. All contractor analysts

provided via this SOW shall possess a clearance appropriate for the work being done and clearance requirement of the assigned work site.

Key personnel must possess active Top-Secret clearances at time of award with the provision that personnel will acquire SCI in the future as directed by the Government per work requirement.

Upon entry, all contractors provided via this SOW shall be CVI Authorized Users, PCII Authorized Users, and have Derivative Classification and Marking training (if they have a Top-Secret Clearance requirement).

The government shall specify that some users will also be users of the Homeland Infrastructure Foundation-Level Data, CISA Gateway (formerly IP Gateway), Homeland Security Information Network (HSIN), Homeland Secure Data Network (HSDN), C-LAN, NCC LAN, and others DHS or CISA networks.

3.3 (U) CONTRACTOR TRAINING

The contractor shall be capable of providing the broad range of technical support services and personnel that remain current with emerging technologies. The contractor staff shall have all the training, expertise, and experience necessary to perform the services specified in the SOW. The contractor shall provide staff training to maintain staff skills current and up to date. The Government will not allow costs, nor reimburse costs associated with the Contractor training employees in attaining and/or maintaining minimum personnel qualification requirements of this contract.

3.4 (U) CONTINUITY OF SUPPORT

The Contractor shall ensure that the contractually required level of support for this requirement is continually maintained. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

3.5 (U) KEY PERSONNEL

The Contractor shall provide the Key Personnel that will be identified in this SOW. Key personnel are expected to be dedicated to the effort, be available on-site seventy-five percent (75%) of the time, and possess active TS clearances at time of award. All key personnel shall be full-time employees of the prime contractor or a subcontractor team member at the time of contract award.

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 calendar days in advance, submit a written justification for replacement, and provide the name and qualifications of any proposed substitute(s) via a resume submission. All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced. The Contractor shall not replace *Key* Contractor personnel without prior written approval from the Contracting Officer.

The Government reserves the right to review resumes of key personnel candidates prior to their assignment. The Government shall not pay any costs associated with removing existing key personnel from the project. The Contractor shall provide a resume for each designated key personnel member. Individual resumes shall be no more than 2 pages in length.

The following positions are to be designated as Key Personnel positions:

- Program Manager
- National Plan Implementation Lead
- Data and Information Sharing PMO Lead
- Strategic Policy and Planning Lead

3.5.1 (U) Program Manager

(U) The Contractor shall provide a Program Manager who shall be responsible for all Contractor work performed under this SOW, including coordination of any Surge work requested by the Government under Task 2.5. The Program Manager shall be the single point of contact for the Contracting Officer and the COR. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Program Manager without prior written approval from the Contracting Officer.

(U) The Program Manager must have at least ten (10) years of demonstrated experience managing projects, on a full-time basis, for similar projects of size and scope. The Program Manager shall possess a Project Management Professional (PMP) certification, in good standing, at time of contract award.

3.5.2 (U) National Plan Implementation Lead

(U) The Contractor shall provide a lead analyst who will coordinate all other tasks under Section 2.2. The name of the National Plan Implementation Lead shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the National Plan Implementation Lead without prior written approval from the Contracting Officer.

(U) The National Plan Implementation Lead must have at least ten (10) years of demonstrated relevant experience acting as a senior representative for an organization that develops national-level plans, including at least three years applied to national security or homeland security missions.

3.5.3 (U) Data/Information Sharing PMO Lead

(U) The Contractor shall provide a Data/Information Sharing PMO Lead to coordinate all tasks under Section 2.3. The name of the Analytics Technical lead shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Analytics Technical Lead without prior written approval from the Contracting Officer.

(U) The Data/Information Sharing PMO Lead must have at least ten (10) years of demonstrated experience acting as a senior data analyst, including at least three years applied to national security or homeland security data. The lead must have a degree in the fields of Mathematics, Statistics, or Engineering and a have undertaken more than 24 credit hours of quantitative based coursework (in the fields of mathematics, statistics, or engineering), including at least six credit hours of calculus. The lead should have experience in presenting and communicating the results of analysis to project stakeholders.

(U) The Data/Information Sharing Lead should also have relevant certifications in the field of data science that could include, but are not limited to, Microsoft Certified Solutions Expert (MCSE): Data Management and Analytics, Certified Analytics Professional, Amazon Web Services (AWS) Certified Big Data - Specialty, or SAS Certified Big Data Professional.

(U) Additionally, preferred but not required, the Lead shall have demonstrated experience acting as a senior representative for an organization that developed national-level plans or initiatives as they relate to data and information sharing including at least three years applied to national security or homeland security missions.

3.5.4 (U) Strategic Policy and Planning Lead

(U) The Contractor shall provide a Strategy, Policy and Planning Lead who will coordinate all tasks under Section 2.4. The name of the Strategic Policy and Planning Lead shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the National Plan Implementation Lead without prior written approval from the Contracting Officer.

(U) The Strategic Policy and Planning Lead must have at least ten (10) years of demonstrated experience acting as a senior representative for an organization that developed national-level plans, including at least three years applied to national security or homeland security missions.

(U) The Strategic Policy and Planning Lead must have at least five (5) years of demonstrated strategy, policy, and planning experience for the Federal government, including at least three years applied to national security or homeland security missions.

3.6 (U) EMPLOYEE IDENTIFICATION

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

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status

is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

3.7 (U) EMPLOYEE CONDUCT

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

3.8 (U) REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

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

4. (U) OTHER APPLICABLE CONDITIONS

4.1 (U) SECURITY

In support of SOW tasks under 2.2, Contractor access to sensitive and classified information is required under this SOW (including access to the National Critical Infrastructure Prioritization Lists, other classified documents, and classified meeting spaces). The maximum level of classification is Top Secret/SCI. Additionally, classified information access is required up to the TS/SCI level at the contractor location. Details will be specified in a Department of Defense (DD) Form 254.

- Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 21 1-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or

- Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or Sensitive but Unclassified Information (SBU) -For Official Use Only -, which consists of any other information which:
  - If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature.
  - Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."

- Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy

to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy.

Prior to performance on this contract all Contractor employees performing work via this SOW (Tasks 2.1-2.3) shall become Chemical-terrorism Vulnerability Information (CVI) and Protected Critical Infrastructure Information (PCII) Authorized Users. Furthermore, contract employees shall be trained on Safeguarding Information and Protected Critical Infrastructure Information. Note, any training and certifications required prior to performance shall be accomplished on-line through web sites the ISD COR will provide the Contractor. Subsequently, the COR will ensure these requirements are met before a staff member starts work on the contract.

4.2 (U) POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

- Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.
- Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigation s will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:
    a. Standard Form 85P, "Questionnaire for Public Trust Positions"
    b. FD Form 258, "Fingerprint Card" (2 copies)
    c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
    d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Rep01is Pursuant to the Fair Credit Reporting Act"

- Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.
- DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.

- Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.
- The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.
- When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).
- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- The POC at the Security Office is:

  DHS Office of Security
  Personnel Security Staff
  [redacted]

4.3 (U) PERIOD OF PERFORMANCE

(U) The period of performance for this contract consist of a six-month base period and three (3) 12-month option periods as follows:

(U) The information in the following table is UNCLASSIFIED:

Performance Period	Performance Period Dates
Base Period	09/15/2022 – 03/15/2023
Option Period One	03/16/2023 – 03/15/2024
Option Period Two	03/16/2024 – 03/15/2025
Option Period Three	03/16/2025 – 03/15/2026

4.4 (U) PLACE OF PERFORMANCE

(U) The primary place of performance will be the Government's facility located at 1310 North Courthouse Road, Arlington, VA. Additionally, work may also be performed at DHS Sensitive Compartmented Information Facilities (SCIF) located at 1110 North Glebe Road, Arlington, VA, and 1616 Fort Myer Drive, Arlington, VA. Other facilities include 4200 Wilson Blvd, Arlington, VA. Other Government facilities within the Department of Homeland Security, in the Washington Metro Area, may also be identified.

(U) Support for meetings in other Washington Metro Area facilities, both governmental and nongovernmental, may be required. Occasional travel to meetings outside the Washington Metro Area may be required. Performance at contractor facilities may be requested based on space availability.

(U) Classified performance at contractor facilities within the Washington Metro Area may be requested dependent on CISA facility space constraints. Please refer to section 4.1 for additional security requirements.

4.5 (U) CONTRACTOR EMPLOYEE ACCESS

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

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

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

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

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

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

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

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

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

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

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

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is 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 the DHS Component. 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.

4.6 (U) CONTRACTOR TELECOMMUTING – REMOTE PERSONAL RESIDENCE WORK LOCATIONS.

(U) Situational telecommuting will be permissible in performance of this requirement. Conditions for situational telecommuting include circumstances such as inclement weather, office closures, etc. Oversight of telecommuting employees shall be in accordance with contractual requirements and the Telecommuting Plan, which will be

provided by the contractor. The Telecommuting Plan should ensure that telecommuting worksites do not include public locations such as libraries, food establishments, parks, or other public locations. All labor categories and personnel are eligible.

(U) All contractor employees and/or subcontractor employees identified for situational telecommuting must complete the annual Computer Security Awareness Training (CSAT) requirement and submit a Telecommuting Agreement through the designated Contracting Officer Representative (COR), if it was not included with the contractor's proposal.

(U) Telecommuting shall not commence until the Telecommuting Agreement has been approved by the contractor's Project Manager and a copy of the approved Agreement provided to the COR. (For Security guidance, see HSAM 3004, Safeguarding Classified Information Within Industry; POPs 302 and 318 or OPOAM Appendix A, Contractor Security Procedures Guide, Parts I and II.).

(U) Contractor and/or subcontractor employees shall not telecommute on Federal holidays, other non-workdays, or in the case of a pandemic or other emergency or unforeseen situation such as an epidemic, natural disaster, early closing, or delayed opening of the Government, as well as a Government shutdown without prior written approval of the COR.

4.7 (U) CONTRACTOR LABOR RATES CHARGED WHILE TELECOMMUTING

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

4.8 (U) HOURS OF OPERATION

4.8.1 Steady State Operations (normal day-to-day operations)

Contract employees shall typically work eight hours a day between the hours of 0700-1800 local time Monday through Friday during Steady State operations (except Government holidays). All Contract employees shall be present during the Core Hours of 0900-1500 Monday through Friday.

If Contractor personnel are unable to physically report to their duty station due to sick leave, annual leave, religious time off, inclement weather, or for any other reason, the Contractor's PM shall notify the COR and the Federal Lead prior to the start of the assigned work hours.

4.8.2 Non-Steady State Operations

A capability to respond after hours (e.g., weekends, holidays) shall be provided that fulfills requirements under this SOW. These after-hour instances will occur approximately 20 times a year usually in response to short suspense on Executive Level Taskers or as a result of a significant incident. In addition to these situations, all Contractor Analysts assigned shall be available for other support requirements as well to include Special Events, incidents, exercises, and other events as agreed upon by Management, COR, and PM. The Contractor shall manage available hours and funding to meet these requirements when apprised by the Government. The Government does acknowledge that during these periods fewer Contractor personnel than normal steady-state operations will be needed at their duty stations, so no Contractor works more than 40-hours per week. The Contractor shall provide the Government with a Weekend/Holiday Shift Schedule before the beginning of each calendar month, so the Government knows who is on-call to respond.

If Office of Personnel Management (OPM) announces, "Federal Offices are Closed in the National Capital Region- Emergency and Telework-Ready Employees Must Follow Their Agency's Policies," Contractor personnel are expected to Telework.

4.8.3 Federal Holidays

The federal government will be closed on the following holidays:

- (U) New Year's Day
- (U) Martin Luther King Day
- (U) Presidents' Day
- (U) Memorial Day
- (U) Juneteenth
- (U) Independence Day
- (U) Labor Day
- (U) Columbus Day
- (U) Veterans' Day
- (U) Thanksgiving
- (U) Christmas

4.9 (U) TRAVEL

Contractor travel will not be required to support this requirement. Local travel will not be reimbursed. Local travel is defined as travel within a 50-mile radius of Washington, DC.

4.10 (U) POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 15 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and to review the Contractor's project management plan. The Post Award Conference will be held at the Government's facility, located at 1310 N. Courthouse Road, Arlington, VA or via teleconference.

4.11 (U) PROJECT PLAN

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 10 business days after the Post Award Conference.

4.12 (U) BUSINESS CONTINUITY PLAN

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 5 business days after the Post Award Conference and shall be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support

during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- A description of how the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
    - Telephone numbers
    - E-mail addresses

Individual event BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 8 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the Contractor PM shall immediately contact the COR to ascertain the status of any Contractor personnel who were located in Government-controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g., email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

The Government and Contractor PM shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. The Contractor shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

4.13 (U) PROGRESS REPORTS

(U) The Project Manager shall provide a weekly progress report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

(U) No later than 10 days after the end of each month, the Project Manager shall provide a Monthly Report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs

by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

4.14 (U) PROGRESS MEETINGS

The PM shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues. These meetings shall take place at the contractor facility, the DHS facility (1301 N Courthouse Rd, Arlington VA), or via teleconference.

The Contractor shall present the monthly report on a monthly basis during the monthly status report update meeting.

4.15 (U) GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

4.16 (U) INTELLECTUAL PROPERTY

Generally, all scripts, tools, data, map templates, symbology, documents, etc. created or obtained by the contractor to perform work on these tasks shall be made available to DHS to use as necessary, unless restricted by law, copyright, or government policy.

All designs, drawings, specifications, notes, and other works developed in the performance of this contract shall become the sole property of the Government and may be used on any other design or construction without additional compensation to the Contractor. The Government shall be considered the "person for whom the work was prepared" for the purpose of authorship in any copyrightable work under 17 U.S.C. 201(b). With respect thereto, the Contractor agrees not to assert or authorize others to assert any rights nor establish any claim under the design patent or copyright laws. The Contractor for a period of three (3) years after completion of the project agrees to furnish all retained works on the request of the Contracting Officer. Unless otherwise provided in this contract, the Contractor shall have the right to retain copies of all works beyond such period.

4.17 (U) PROTECTION OF INFORMATION

Contractor access to CVI, PCII, and proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information and other applicable Government laws, Policies and Regulations. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The

Contractor shall not release Government furnished information, data, and documents to outside parties without the prior and explicit consent of the Contracting Officer.

The Contractor will follow all applicable DHS security requirements and laws and regulations for handling, generating, and transmitting both classified and sensitive but unclassified (SBU) information. Reference materials include, but are not limited to, the following:

1. DHS 4300a Policy. Components shall require contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in accordance with NIST SP 800-27, Engineering Principles for Information Technology Security.
2. DHS 4300B Policy. DHS 4300B is the requirements set forth for National Security Systems.
3. DHS Security Classification Guidance – IP – 003, March 2007
4. Safeguarding Classified National Security Information: Reference Pamphlet, February 2004
5. Safeguarding Sensitive But Unclassified (For Official Use Only) Information, MD 11042, May 11, 2004
6. Protected Critical Infrastructure Information (PCII) Procedures Manual, February 17, 2004.
7. Chemical-terrorism Vulnerability Information (CVI) Procedures Manual, June 2007.

4.17.1 Non-Disclosure of Chemical-Terrorism Vulnerability Information

The Contractor shall comply with all requirements of 6 U.S.C., 621 et seq, as amended, any properly promulgated implementing regulations, and in the DHS Procedures Manual as they may be amended from time to time and shall safeguard CVI in accordance with the procedures contained therein.

The Contractor shall ensure that each of its employees, consultants, and subcontractors who require access to because they have a need to know, are CVI Authorized User. The contractor agrees that none of its employees, consultants or subcontractors will be given access to CVI without having previously executed an NDA and understand the requirements for safeguarding CVI as documented in the CVI Procedural Manual.

4.17.2 Non-Disclosure of Protected Critical Infrastructure Information (PCII):

The following PCII guidelines, issued by the DHS PCII Program Office, will be followed:

The parties agree to implement the Final rule promulgating regulations at Title 6 Code of Federal Regulations Section 29 to govern procedures for handling critical infrastructure information. The regulations detailed in the Final rule, which was effective upon publication pursuant to Section 808 of the Congressional Review Act, were promulgated pursuant to Title II, Section 214 of the Homeland Security Act of 2002, known as the "Critical Infrastructure Information Act of 2002" (CII Act).

The Contractor shall not request, obtain, maintain or use Protected Critical Infrastructure Information (PCII) without a prior written certification from the PCII Program Manager or a PCII Officer that conforms to the requirements of Section 29.8(c) of the Final Rule.

The Contractor shall comply with all requirements of the PCII Program set out in the CII Act, in the implementing regulations published in the Final Rule, and in the PCII Procedures Manual as they may be amended from time to time and shall safeguard PCII in accordance with the procedures contained therein.

The Contractor shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed Non-Disclosure Agreements (NDAs) in a form prescribed by the PCII Program Manager and agrees that none of its employees, consultants or sub-contractors will be given access to PCII without having previously executed an NDA.

The Contractor's employees requiring access to PCII will complete all required PCII training and sign the DHS PCII Non-Disclosure Agreement (NDA) prior to having access to PCII. The Contractor agrees that none of its employees, consultants or subcontractors will be given access to PCII without having previously executed the NDA.

The Contractor's contractors, subcontractors, and consultants are not authorized to disseminate controlled unclassified information (CUI), CVI or PCII without adherence to the specific program safeguarding and handling requirements and outside of the Contractor's prior authorization from COR and then only when all persons with access to the information are authorized users who have signed non-disclosure agreements.

4.17.3 SAFEGUARDING OF SENSITIVE INFORMATION

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

(b) *Definitions.* As used in this clause—

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

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

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

Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

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

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A (Version 13.1, July 27, 2017)
(3) DHS 4300A Sensitive Systems Handbook (Version 12.0, November 15, 2015) and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A (Version 13.1, July 27, 2017)* and the *DHS 4300A Sensitive Systems Handbook* (Version 12.0, November 15, 2015) provide the policies and procedures on security for Information Technology (IT) resources. *The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the

names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

(1) *Complete the Security Authorization process.* The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 13.1, July 27, 2017), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 12.0, November 15, 2015), or any successor publication, and the *Security Authorization Process Guide* including templates.

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

Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.* The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

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

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

1. Data Universal Numbering System (DUNS);
2. Contract numbers affected unless all contracts by the company are affected;
3. Facility CAGE code if the location of the event is different than the prime contractor location;
4. Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
5. Contracting Officer POC (address, telephone, email);
6. Contract clearance level;
7. Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
8. Government programs, platforms or systems involved;
9. Location(s) of incident;
10. Date and time the incident was discovered;
11. Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
12. Description of the Government PII and/or SPII contained within the system;
13. Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
14. Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

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

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

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

- Inspections,
- Investigations,
- Forensic reviews, and
- Data analyses and processing.

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

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

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

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

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

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

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

- Triple credit bureau monitoring;
- Daily customer service;
- Alerts provided to the individual for changes and fraud; and

- Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

- A dedicated telephone number to contact customer service within a fixed period;
- Information necessary for registrants/enrollees to access credit reports and credit scores;
- 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;
- Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
- Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

4.17.4 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING

(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.

(c) *Privacy Training Requirements*. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

4.18 (U) SECTION 508 REQUIREMENTS

Section 508 Compliance

1. Section 508 Requirements (include in the SOW, PWS, or SOO)

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.

1.1 Section 508 Requirements for Technology Services (include in the SOW, PWS, or SOO)

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 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.

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

1.2 Section 508 Deliverables (include in the SOW, PWS, or SOO)

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

DHS Enterprise Architecture Compliance

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

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

DHS Geospatial Information System Terms and Conditions

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (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.

DHS Cyber-Supply Chain Risk Management (C-SCRM) Terms & Conditions

The offeror shall comply with the most current version of the DHS Cybersecurity Supply Chain Risk Management terms and conditions. (If the DHS C-SCRM T&Cs reference is not publicly accessible then the most current language will be added to this section of the SOW by the contracting officer prior to solicitation release)

EPEAT and Energy Star Language

"All hardware procured directly or in support of this action must meet applicable and appropriate Electronic Product Environmental Assessment Tool (EPEAT) and ENERGY Star standards."

5. GOVERNMENT TERMS & DEFINITIONS

- (U) A-LAN – DHS unclassified network
- (U) CFATS – Chemical Facility Anti-Terrorism Standards
- (U) C-LAN – DHS classified network
- (U) CI – Critical Infrastructure
- (U) CISR – Critical Infrastructure Security and Resilience
- (U) CONUS – Continental United States
- (U) COP – Common Operating Picture
- (U) COR – Contracting Officer's Representative
- (U) CVI – Chemical-terrorism Vulnerability Information
- (U) DHS – Department of Homeland Security
- (U) EOD – Entry on Duty
- (U) FEMA – Federal Emergency Management Agency
- (U) GEOINT- Geospatial Intelligence
- (U) GSA- General Services Administration
- (U) GST – Geospatial Support Team
- (U) GMO – Geospatial Management Office
- (U) GII – Geospatial Information Infrastructure
- (U) GIS – Geographic Information System
- (U) HILFD – Homeland Infrastructure Foundation-Level Database
- (U) HSDN – DHS secret network
- (U) IVP – Infrastructure Visualization Product
- (U) NCR – National Capital Region
- (U) NIPP- National Infrastructure Protection Plan
- (U) NRMC – National Risk Management Center
- (U) NSSE – National Security Special Event
- (U) OPM – Office of Personnel Management
- (U) PCII – Protected Critical Infrastructure Information
- (U) PM – Project Manager
- (U) PMO – Project Management Office
- (U) PSA – Protective Security Advisor
- (U) PWS – Performance Work Statement
- (U) SOW – Statement of Work
- (U) QC – Quality Control
- (U) RFI – Request for Information
- (U) RRAP – Regional Resiliency Assessment Program
- (U) RD – Regional Directors
- (U) RS – Remote Sensing
- (U) SEAR – Special Event Assessment Rating
- (U) SOP – Standard Operation Procedure
- (U) SSE – Special Security Events

6. GOVERNMENT FURNISHED RESOURCES

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

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

Government property has been inspected for compliance with the Occupational Safety and Health Act (OSHA). No hazard has been identified for which a work-around has been established. Should a hazard be subsequently identified, the Government will correct OSHA hazards accordingly to Government developed and approved plans of abatement taking into account safety and health priories. A higher priority for correction will not be assigned to the property provided hereunder merely because of this contracting initiative. The fact that no such conditions have been identified does not warrant or guarantee that no possible hazard exists, or that work-around procedures will not be necessary or that the property as furnished will be adequate to meet the responsibilities of the Contractor. Compliance with the OSHA and other applicable laws and regulations for the protection of employees is exclusively the obligation of the Contractor. Further, the Government will assume no responsibility for the Contractor's compliance or noncompliance with such requirements, with the exception of the aforementioned requirement to make corrections according to approved plans of abatement subject to base-wide priorities. Before any modification of the property performed by the Contractor at his or her expense, the Contractor shall furnish the Contracting Officer documentation describing, in detail, the modification requested. No alterations to the property shall be made without specific written permission from the Contracting Officer. In the case of alterations necessary for compliance with OSHA, such permission will not be withheld. The Contractor shall return the property to the Government in the same condition as received, fair wear and tear and approved modifications excepted. The property shall only be used in performance of this contract.

6.1 PROPERTY INVENTORY

CISA/ISD must establish and maintain an accurate master inventory of all property purchase for CISA under this contract. As such, this section is only applicable if property is purchased exclusively for use under this contract.

6.2 MONTLY ASSET MANAGEMENT REPORT

CISA/ISD will ensure personnel prepare a monthly Asset Management Report, which contains accurate information for all CISA property located at their facility. At a minimum, this report must include:

- (U) DHS Barcode
- (U) Acquisition Date
- (U) Acquisition Status
- (U) Asset Condition
- (U) Manufacturer Name
- (U) Manufacturer Model
- (U) Asset Description
- (U) Serial Number
- (U) Asset Cost
- (U) Location

7. (U) INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per Section VII, Contract Clauses; Paragraph A. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR Clause 52.232-25 Prompt Payment, and FAR Clause 52.232-7, Payments under Time and Materials and Labor-Hours. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) (U) Cover sheet identifying DHS;
2) (U) Task Order Number;
3) (U) Modification Number, if any;
4) (U) DUNS Number;
5) (U) Month services provided;
6) (U) CLIN and Accounting Classifications;
7) (U) Contract Line Item Number (CLIN) and description for each billed item; and
8) (U) Any additional backup information as required by this contract.

The contractor shall submit invoices monthly, but no later than the 10th day of each of each month.

The Contractor shall submit the invoice electronically to the address below (ATTN: CISA/OUS)

E-mail: NPPDInvoice.Consolidation@ice.dhs.gov

Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

E-mail: Kerri.Williams@hq.dhs.gov (Contracting Officer) Alana.Nweke@hq.dhs.gov (Contract Specialist)

The contractor shall submit invoices to the email addresses above. Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation. The COR will provide any invoicing templates for consistency of data submission.

If the invoice is submitted without all required back up documentation, the invoice shall be rejected. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval.

8. (U) GOVERNMENT ACCEPTANCE PERIOD

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

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

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

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

9. (U) DELIVERABLES

(U) The Contractor shall consider items in **BOLD** as having mandatory due dates. Items in *italics* are deliverables or events that must be reviewed and/or approved by the COR prior to proceeding to next deliverable or event in this SOW.

(U) The information in the following table is UNCLASSIFIED:

ITEM	SOW SECTION	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.6	**Telecommuting Plan**	10 business days after the Post Award Conference	COR, Contracting Officer
2	4.10	**Post Award Conference**	15 business days after contract award	N/A
3	4.11	**Project Plan**	Post Award Conference	COR, Contracting Officer
4	4.11	**Project Plan**	10 business days after the Post Award Conference	COR, Contracting Officer
5	4.12	**Original Business Continuity Plan**	5 business days after the Post Award Conference	COR, Contracting Officer
6	4.12	**Updated Business Continuity Plan**	Yearly	COR, Contracting Officer
7	4.13	**Progress Reports**	Weekly; Monthly	COR, Contracting Officer
8	6.1	**Master Inventory Report**	Monthly	COR, APO
9	6.1	**Receipts for Purchased CISA Property**	Within 5 Business days of purchase	COR, APO
10	6.2	**Monthly Asset Management Report**	Monthly	COR, APO
11	6.2	**Invoices/packing slips/receipts for property purchased for CISA**	Monthly, with the Asset Management Report	COR, APO

ITEM	SOW SECTION	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
12	2.1, 2.2, 2.3, 2.4, 2.5	**Project Management Plans**	As requested, no later than 10 days after project assignment	APO
13	2.2	**National Plan Implementation Strategy**	Within 30 days of contract award	APO
14	2.2	**National Plan Engagement Strategy / Roadmap**	Within 60 days of contract award	APO
15	2.2	**National Plan Strategic Implementation Plan**	Within 120 days of contract award	APO
16	2.2.2	**Draft National Infrastructure Criticality and Prioritization Approach**	Within 150 days of contract award	APO
17	2.2.2	**National Infrastructure Criticality Plenary Forum Event Plan**	150 days after contract award	APO
18	2.2.3	**National Plan Independent Study Training Course Curriculum**	Within 120 days of contract award	APO
19	2.3	**ISD Data Stewardship Framework**	Within 90 days of contract award	APO
20	2.3	**ISD SPR Data PMO CONOPs**	Within 60 days of contract award	APO
21	2.3	**ISD Data Stewardship Framework**	60 days after contract award	APO
22	2.3	**Data Model, Architecture, and Process for Annual Data Call**	60 days after contract award	APO
23	2.3	**Annual SLTT Data Call**	TBD	APO
24	2.4	**Sector-Specific Plan template and guidance**	45 days after contract award	APO
25	2.4	**Intelligence and Information Sharing Annex to National Plan**	150 days after contract award	APO
26	2.4	**National Critical Function Annex to National Plan**	150 days after contract award	APO
27	2.4	**"Plan in a Box" Template for SLTT Critical Infrastructure Protection Program Model**	150 days after contract award	APO

ITEM	SOW SECTION	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
28	2.4	**Draft PPD-21 Policy Revision**	180 days after contract award	APO
29	2.2, 2.5	**Provide policy, strategy, and planning support for exigent products**	As requested	APO

TRANSITION PLANNING

In the event that responsibility for fulfillment of the tasks described in this SOW, either in whole or in part, is transferred to a new contractor or the government, the contractor shall participate in transition meetings with the program manager, project staff, and representatives of the successor Contractor and/or government personnel. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition in contractor support.

Further, and as instructed by the COR, the contractor shall develop a *Transition Out Plan*, which the contractor shall develop, document, and monitor the execution of a transition-out activities that may be used to transition related tasks and materials described in this SOW to a new contractor, or to the government. The plan shall incorporate an inventory of all services and materials required to fully perform the contract requirements. The plan shall include a schedule of briefings, including dates, times, and resources allotted, that will be required to fully transition all materials developed to the follow-on contractor, and shall provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan is to ensure that the follow-on contractor, or the government, will be provided sufficient information and be fully briefed prior to the current expiration date of the contract, to provide adequate time for the new contractor to have their personnel completely familiar with the requirements and in place on the turnover date. The contractor shall plan for up to a 90-day transition period. The plan shall provide the contact information for contractor individuals who will be assigned to the transition team and identify their roles in the transition.

The plan shall also identify the actions, plans, personnel, procedures, deliverables, work products, and timelines by task area necessary to ensure a smooth transition from contract start date to full operational status by new contractor, or to the government. The plan will incorporate an inventory of all services and materials developed that will be required to fully perform the services provided under this requirement. The plan will include a schedule of briefings, including dates and time and resources allotted, that will be required to fully transition all materials developed to the follow-on contractor.