DEPARTMENT OF HOMELAND SECURITY
Cybersecurity and Infrastructure Security Agency
Integration Operations Division

Planning, Exercise, Readiness & Training (PERT)

Statement of Work

UNCLASSIFIED/PROCUREMENT SENSITIVE

Contents

1.0 GENERAL

The threats our Nation faces—digital and physical, man-made, technological, and natural—are more complex, and the threat actors more diverse, than at any point in our history. Our Nation's well-being relies upon secure and resilient critical infrastructure—those assets, systems, and networks that underpin the American way of life. The partnership among owners and operators; Federal, State, local, tribal, and territorial governments; regional entities; non-profit organizations, academia and the international community are key to managing the risks to critical infrastructure. CISA is at the heart of mobilizing a collective defense as we lead the Nation's efforts to understand and manage risk to our critical infrastructure.

CISA's partners in this mission span the public and private sectors. Programs and services CISA provide are driven by CISA's comprehensive understanding of the risk environment and the corresponding needs identified by our stakeholders. The Agency seeks to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

To achieve this mission, CISA requires effective coordination and collaboration among a broad spectrum of government and private sector organizations. CISA builds the national capacity to defend against cyber-attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies. CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors and deliver technical assistance and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide. CISA enhances public safety interoperable communications at all levels of government to help partners across the country develop their emergency communications capabilities. Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of a natural disaster, act of terrorism, or other man-made disaster.

CISA performs its mission through a matrixed organizational agency, comprised of three primary disciplines – Cyber Security Division (CSD), Emergency Communication Division (ECD), and Infrastructure Security Division (ISD) supported by three cross-cutting divisions - Stakeholder Engagement Division (SED), National Risk Management Center (NRMC), and Integrated Operations Division (IOD).

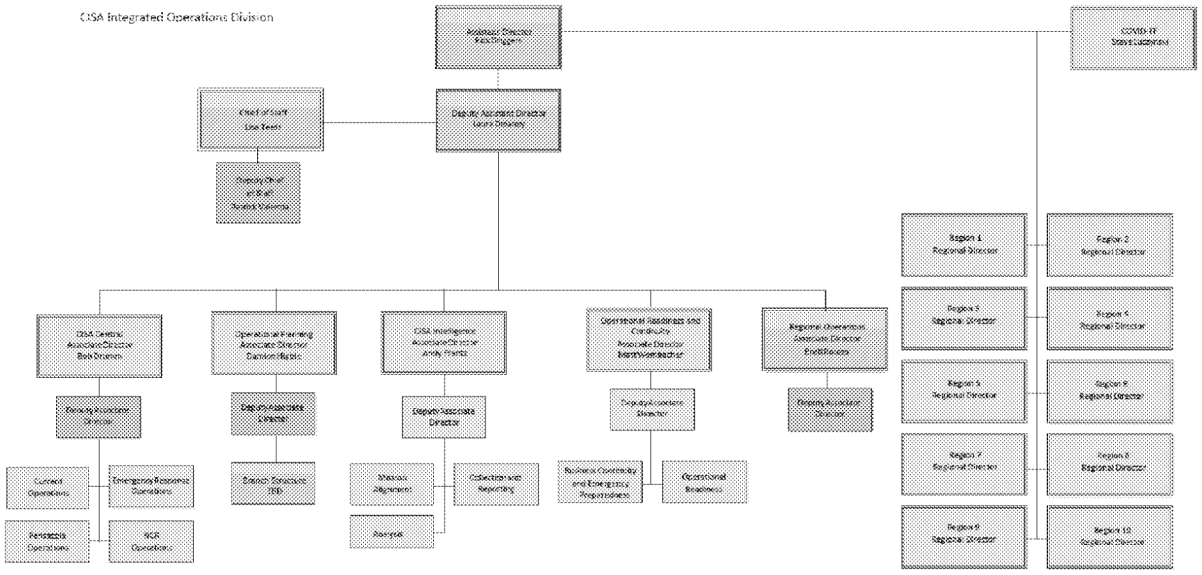
2.0 PURPOSE

This Statement of Work (SOW) describes the support needed for IOD to achieve and mature its operational planning and readiness mission set, specifically establishing a continuous cycle of planning, organizing, evaluating, and taking corrective action to ensure effective coordinated activities to support cyber defense and incident response operations and response to natural and man-made disasters. The mission set and requirements contained in this SOW are required during

steady state and times of heightened activities due to the evolving threat landscape or response to natural disasters.

CISA's organizational construct is centered on unifying all parts of the Agency to best meet its mission. Given the diverse array of stakeholders and capabilities across the cybersecurity, emergency communications, and infrastructure security domain, strong operational documentation is critical to ensure standardization of operational procedures.

IOD was established to coordinate, collaborate, and execute CISA's operational and planning activities while ensuring seamless support to stakeholder's critical needs. IOD works with intelligence partners to ensure focus on CISA priorities and delivers intelligence products and context to support all missions. Additionally, IOD serves as the primary service delivery function for CISA customers, operating under the direction of the ten regional directors. IOD coordinates with other divisions on implementation of programs in the field.



The work described in this SOW primarily falls under the purview of the Operational Planning (OP) and Operational Readiness, and Continuity (ORC) sub-divisions. The OP and ORC develop operational plans in support of CISA's cyber defense and incident response activities as well as CISA's activities in support of man-made and/or natural disasters. Responsibilities executed by OP include developing operational plans, operational planning standards, and internal Standard Operating Procedures (SOPs) and exercises.

3.0 SCOPE

The scope of this SOW includes services associated with IOD's operational planning activities in support of IOD's mission areas, including: incident management and reporting; training and exercising/verification of plans; information gathering/collection, reporting, and analysis; and regional operations, including the creation of professional graphic images which enhance planning, exercise, and operational documentation. Operational planning activities include development and refinement of:

- Steady-state, contingency, and crisis-action operational plans,
- Concepts of Operations (CONOPS),
- SOPs,
- Checklists supporting plans and operations, internal training, and internal and external exercise support documents,
- Templates and standards related to operational plans and doctrine.

All operational planning documents will be developed in accordance with the CISA Governance Framework or as directed by IOD.

4.0 BACKGROUND

In 2018 the Cybersecurity and Infrastructure Security Act was passed, creating a new Agency within DHS titled the Cybersecurity and Infrastructure Security Agency (CISA).

In April of 2020, CISA's Strategy, Policy, and Plans released the CISA Governance Framework, which provides the structure within which policies, plans, and doctrine are established, implemented, communicated and continuously monitored. The CISA Governance Framework is made up of four pillars, of which the CISA Integrated Planning System provides the principles, approach, structure, relevant standards and processes that guide the development of integrated and complimentary plans across CISA.

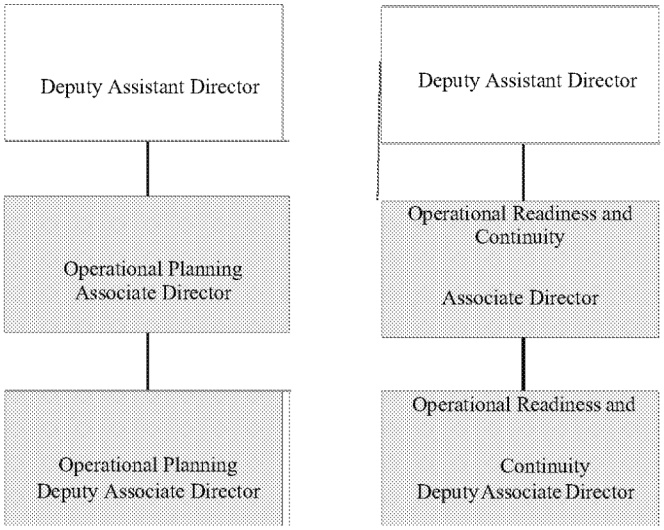
The Integrated Operation Division was created to ensure CISA-wide operational activities are coordinated, collaborative, and transparent across the agency. IOD leads and coordinates CISA's operational planning activities. OP and ORPC's functions are integral to the successful execution of IOD's mission, as they are responsible for developing, maintaining, training, and exercising CISA's operational plans. These sub-divisions follow the CISA Governance Framework and processes to lead the development of plans that reflect CISA Leadership Strategies and priorities and also incorporates the unique capabilities, roles, and responsibilities of each of the CISA divisions and lines of business. As part of the operational readiness function, ORC is responsible for CISA's continuity of operations planning, testing, and training across CISA. IOD must unify operational coordination, improve management of operational activities across CISA, including the regions, and rapidly and effectively respond and report.

For those familiar with the previous NPPD organizational construct, IOD is comprised of: 1) the former NPPD watch functions that were associated with the National Cybersecurity and Communications Integration Center (NCCIC), National Infrastructure Coordinating Center

(NICC), and National Coordinating Center for Communications (NCC); 2) operational planners that were associated with the NICC; 3) emergency support functions residing in NCC (ESF #2) and ISD (ESF #14); 4) intelligence analysis functions that resided in the NRMC; and, 5) continuity of operations functions that resided in the NPPD Front Office. The largest change as part of the ongoing CISA 2020 reorganizational efforts, relate to the alignment of all CISA field staff under ten Regional Directors who report to IOD leadership. The alignment of all field personnel encompasses protective security advisors, cybersecurity advisors and the regulatory chemical security inspectors that play an integral part in identifying and regulating high-risk chemical facilities to ensure they have security measures in place that reduce the risk of certain hazardous chemicals being weaponized.

Most of the work described in this SOW primarily pertains to the mission objectives of the IOD sub-divisions titled Operational Planning (OP) and Operational Readiness and Continuity (ORC). These sub-divisions combine the legacy NICC Planning and Readiness / Preparedness capabilities and the Business Continuity and Emergency Preparedness (BCEP) capabilities of legacy NPPD BCEP. OP and ORC are integral to making IOD and CISA successful by ensuring all CISA operational plans are developed in a collaborative fashion, tested, trained and exercised to help mature the organization. Operational Planning operates in the National Capitol Region (NCR) but may travel to the Regions. ORC operates within the NCR, the Mount Weather Emergency Operations Center (MWEOC) Continuity of Operations (COOP) site, Denver, CO, and Pensacola, FL, and may have to travel to other CISA locations to perform COOP, Reconstitution, or Devolution activities. Both sub-divisions serve in all operational environments, from steady state to no-notice incidents or emergencies, in extremely time-sensitive environments, and during periods of severe weather and government shutdowns.

Operational Planning **Operational Readiness and Continuity**



These sub-divisions maintain a continuous cycle of planning, organizing, training, exercising, evaluating, and taking corrective action to ensure effective coordination and information sharing across CISA's operations. This cycle is one element of a broader National Preparedness System to prevent, respond to, and recover from natural disasters, acts of terrorism, and other disasters and supports CISA's responsibilities outlined in the National Cyber Incident Response Plan and CISA's efforts to conduct cyber defense operations. The organization builds and promotes a culture of individual and organizational emergency preparedness that enables and exercises the Agency's readiness capabilities to ensure continuous execution of the CISA mission.

While the primary points of contact for this work reside in IOD's OP and ORC sub-divisions, it should be clear that IOD must communicate, collaborate, and develop products with all branches within IOD, across all CISA divisions and mission support elements, and among our many external stakeholders to meet mission requirements.

5.0 APPLICABLE DOCUMENTATION

The following documents provide additional background information that are relevant to the work to be performed under this contract. Copies of these documents can be provided upon request.

- Executive Order 13636: Improving Critical Infrastructure Cybersecurity
- Executive Order 13718: Commission on Enhancing National Cybersecurity
  Presidential Policy Directive 8: National Preparedness
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
- Presidential Policy Directive 41: United States Cyber Incident Coordination
- National Cyber Incident Response Plan (NCIRP) – describes a national approach to dealing with cyber incidents; addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response
- Action Memo: Implementation of CISA 2020 Transformation Initiative and Establishment of New Organizational Elements, dated March 25, 2020 - directs the commencement of full execution of the CISA 2020 implementation plan, to include the establishment of eight (8) new and discrete organizational divisions and offices within CISA.
- Federal Continuity Directives 1 and 2
- Homeland Security Exercises and Evaluation Program (HSEEP)
- CISA Policy and Governance Framework
- FEMA Operational Planning Manual
- DHS Office of Operations Coordination Strategic Plan Fiscal Year 2020 to 2024
- Cybersecurity and Infrastructure Security Agency *2018 Writing Style Guide*, December 2018

6.0 TASKS

The objective of this SOW is to provide highly skilled personnel to support the development and implementation of operational plans, and doctrine; data analytics (metrics and measures) related to steady-state and contingency operational planning, readiness, and continuity functions; and the production of the standards and documentation that institutionalize and operationalize the organization and its capabilities. This SOW Contains 4 required tasks and 2 optional tasks. The optional tasks may be awarded upon confirmation of need and/or availability of funding. The SOW tasks are as follows:

- Task 1: Task Management (Required)
- Task 2: Operational Planning (including metrics and measures) (Required)
- Task 3: Review of National / Interagency, DHS, CISA, and IOD Level Plans (Required)
- Task 4: Readiness (Required)
- Task 5: Surge (Optional)
- Task 6: Operational Planning Support (Optional)

Some contractor staff supporting this contract are required to hold a TS/SCI clearance with DHS fitness. In several cases, contractor staff may only require a Secret clearance with DHS fitness as noted below:

Task 1: Program Manager	TS/SCI
Task 2: Operational Planning Lead	TS/SCI
Technical Editor	Secret
Operational Planners (Mid)	Secret
Operational Planners (Entry)	Secret
Graphics	Secret
Task 3: Operational Planners (Mid)	Secret
Task 4: Training and Exercise Lead SR	TS/SCI
Exercise Planners (Mid)	Secret
Trainers (Mid)	Secret
Task 6: Operational Planners (Mid)	Secret

For Task 1, it is possible for a small number of contractor staff to only hold Public Trust with DHS Fitness. In rare instances, it is possible for a task to be defined that would require no access to DHS IT systems or DHS sensitive information, in which case DHS Fitness would not be required. An example of such a project may be to research National, State, Local Response Plans or State/Local communications plans. In such cases, the approval to proceed without DHS Fitness would be documented and approved by the Contracting Officer Representative (COR).

6.1 Task 1: Task Management

The objective of task management support is to provide the program management, project control, and contract administration necessary to manage the tasking in the contract. Within sixty (60) calendar days, the contractor shall provide the Government with a proposed option(s) to make the subsequent tasks with a recommendation(s) to perform more effectively. After the first ninety (90)

calendar days, the contractor shall continue to provide continuous improvement recommendations as part of the monthly reporting schedule.

The majority of contractor staff supporting Task 1 must have a minimum of a Secret clearance with DHS fitness. It is possible for personnel who support financial tracking or other "back-office" tasks that support contract management to work with Public Trust and DHS Fitness.

6.1.1 Kickoff Meeting

The contractor shall develop a proposed kickoff meeting agenda and provide it to CISA within ten (10) calendar days after award. The contractor shall deliver an electronic copy of their kickoff briefing to the Contracting Officer Representative (COR) at least two (2) business days before the scheduled kickoff. The contractor shall record the minutes and action items from the kickoff meeting. The kickoff briefing shall include the following:

- Introduction of management and technical teams.
- Presentation of all deliverables (including proposed formats and reporting methods).
- Any other relevant items as introduced at the discretion of the contractor and/or the government.

6.1.2 Monthly Program Management Review (PMR)

The contractor is required to participate in a monthly Program Management Review (PMR) meeting for their contract and to deliver a Monthly Status Report (MSR report) at least two (2) business days prior to the PMR meeting. The contractor shall provide the following information in the MSR which includes, but is not limited to, the following information:

- Contractor's staffing roster (including attrition rates)
- Discussion of the previous month's progress
- Deviance from previous month's planned progress (either positive or negative)
- Current month's planned progress
- Issues and recommendations
- Estimated costs versus actual costs (cost variance)
- Program risks, risk mitigation plans, and risk mitigation actions taken
- Proposed options to perform SOW tasks more effectively, if observed

The MSR will also include all recurring and non-recurring costs, cumulative cost, total labor hours, and cumulative labor hours for each SOW task for the previous month. Current estimates at completion (EACs) shall be incorporated within the MSR and reflect the most up to date EACs at the time of reporting. Additionally, the contractor may be required to deliver additional financial and management reports upon request from the government.

The contractor shall identify contractor personnel who are performing work prior to Entry on Duty (EOD) (for those employees awaiting a determination who are already authorized by the COR to begin work). The report shall include:

- Name of individual
- Performance location
- Start date on contract
- Clearance level
- Requested final EOD approval level
- Date of EOD submission
- Date of COR approval to begin performing unclassified support under this task
- Role of individual
- Explanation of current work being performed while awaiting fitness
- Name of the Government task lead that the individual contractor is supporting

The contractor shall deliver the MSR to the government by the 15th of each month.

The contractor shall meet as required by the government to discuss task management, security requirements, technical documentation, incident response, surge support, and/or other project related status or issues. The contractor shall develop and distribute a meeting agenda prior to the scheduled meeting as requested by the government.

6.1.3 Staffing

The contractor shall include with the submission of their proposal a Draft Staffing Plan that will address how the contractor intends to meet the requirements outlined in the SOW. Forty-five (45) calendar days post contract award, the contractor shall deliver a Final Staffing Plan that includes updates determined necessary following contract transition and an introduction into IOD's operational environment. The Draft and Final Staffing Plans will address the requirements needed to perform the work contained within this SOW.

The contractor shall have 75% of its personnel submitted for their appropriate fitness and security reviews within sixty (60) calendar days of contract award and 90% of its personnel submitted for their appropriate fitness and security reviews within one-hundred (100) calendar days of contract award.

The Government considers retention and proficiency training key elements critical to the success of IOD's mission. Understanding the contractor's approach to retaining and training staff is important, and therefore should also be included in the Draft and Final Staffing Plans. Specifically, the contractor shall address:

- How proficiency training will be accomplished
- How retention levels will be maintained
- How turnover will be reduced

The contractor shall ensure that its staff and subcontractors maintain any generally required professional certifications, accreditations, and proficiency relative to their areas of expertise. The contractor should retain documentation of such records. The government will not pay expenses to meet this requirement.

6.1.3.1 Staffing Plan

The contractor shall include with the submission of their proposal a Draft Staffing Plan that will address how the contractor intends to meet the requirements outlined in the SOW. Forty-five (45) calendar days post contract award, the contractor shall deliver a Final Staffing Plan that includes updates determined necessary following contract transition and an introduction into IOD's operational environment. The staffing plan will address the requirements needed to perform the work on the contract and shall include the following information:

- Contractor organizational constructs and linkages between IOD's team structure
- Labor category descriptions/qualifications proposed.
- Percentage of personnel currently available by labor category by applicable task.
- Percentage of personnel currently available by labor category with TS/SCI personnel security clearances.
- Proposed approach for supporting surge requirements.
- Corporate retention rates (%) for staff in the Washington, DC, metropolitan area.

The contractor staffing plan will also address their ability to ensure that personnel maintain ongoing knowledge of operational planning, readiness (training and exercises), and continuity of operations.

6.1.3.2 Key Personnel

This contract requires 2 contractor staff to be designated as key personnel. The contractor shall propose resumes for key personnel that adequately demonstrate the individual's abilities to meet the requirements of those positions. The same person may not be proposed in multiple roles. The knowledge, skills, and abilities for the relevant specialty areas and work roles should meet the guidance and criteria for operational planning as noted in resources such as the DHS Overview of Federal Agency Operational Plans, understanding that the majority of effort will be placed not on Strategic Planning (concentrated towards attaining the long-term objectives), but on operational planning to achieve short-term objectives of the Integrated Operations Division - these being used to set priorities and align the resources in such a way that leads to the accomplishment of the Division's goals.

Unless otherwise noted, the designated key personnel must be available during normal core hours (defined as 0800-1600) to meet with CISA (in person or as otherwise agreed upon by CISA) to discuss tasks and address problems should they arise. In the event of disaster recovery or continuity of operations plan (COOP) events, key personnel shall be available during core hours of operation and during periods of no-notice emergencies, including localized acts of nature,

accidents, and military or terrorist attacks, to plan, direct, and control the overall management and operational functions specified herein..

All proposed key personnel substitutions should be submitted, in writing, to the CO at least thirty (30) days prior to the proposed effective date of substitution. Each request must provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume for the proposed substitution, information regarding the full financial impact of the change, and any other information required by the CO to approve or disapprove the proposed substitution. Where possible, if key personnel, for whatever reason, become unavailable for work under the contract for a continuous period exceeding thirty (30) calendar days or are expected to devote substantially less effort to the work than indicated in the proposal, the contractor shall propose a substitution to meet the government's key personnel requirements.

The contractor agrees that, unless otherwise stated in the contract, during the first 120 calendar days of the contract, no key personnel substitutions or additions shall be made unless necessitated by compelling reasons including, but not limited to: an individual's illness, death, termination of employment, declining an offer of employment (for those proposed as contingent hires), or family-friendly leave. In such an event, the contractor must promptly provide the information required by the paragraphs below to the CO for approval prior to the substitution or addition of key personnel.

All proposed key personnel should demonstrate experience of similar size and scope of the requirements outlined within this SOW and in accordance with OASIS SB Labor Categories Experience and Qualification (E&Q) levels. Below are required key personnel duties, qualifications and certifications:

(One) Program Manager (PM): The PM must have excellent knowledge of performance evaluation and change management principles and excellent communication, problem solving, and leadership skills. The PM is responsible for organizing all services pertaining to this contract. The PM shall be tasked with fulfilling staffing plans; providing strategic guidance to multiple teams; formulating, organizing, and monitoring inter-connected projects; preparing and/or presenting reports to government PMs; and fulfilling the task management deliverables within this SOW. The PM will also coordinate with other task leads to ensure specific deliverables are being completed within the agreed upon timelines and communicating any discovered risks and mitigation plans with the government. The PM requires an active TS/SCI security clearance and DHS fitness. Candidates with significant experience as a Program Manager (PM) or other managerial positions are preferred. OASIS Senior Level qualification required; Project Management Professional (PMP) or Level I Program Management Acquisition Professional certification preferred.

(One) Operational Plans Lead: The Operational Plans Lead must have proven experience as a planner and writer with either civilian government or military experience. Operational Plans experience includes: the planning process and workflows; development and maintenance of operational documentation; excellent writing and technical editing skills; demonstrated experience writing communications for executive senior leadership and requires an active TS/SCI security clearance with DHS fitness. OASIS Level Senior required.

6.1.4 Schedule Management

For specific initiatives or projects that involve multiple, dependent actions to be completed over a period of time, the contractor may be asked to develop a schedule that clearly documents all key milestone events, tracks schedule variations, identifies completion dates, and critical path activities. Additionally, the schedule shall:

- Contain percent complete, i.e., a percentage value that indicates the current status of a task expressed as the percentage of work that has been completed.
- Contain external dependencies, i.e., a CISA entity or an entity external to the contractor on which a task is dependent.
- Be delivered in Microsoft Project.

The schedule shall be maintained by the contractor in collaboration with IOD. The contractor shall couple the schedule with regular management control meetings to ensure all activities underway are coordinated and support the objectives of the overall project, and contain each activity's name, duration, start date, finish date, predecessors, and successors.

6.1.5 Issue and Risk Management

The contractor shall participate in the issue and risk management activities of IOD by identifying issues (real) and risks (not yet real) to initiatives, projects, and or strategies. The contractor shall analyze issue and risk impacts and identify mitigations to ensure the Government is properly considering such items when making decisions. The contractor shall also assist the Government by working with IOD representatives to identify strategies to resolve issues and mitigate risks, and the contractor shall inform the Government when unable to reach consensus. The contractor shall identify, track, and manage issues and risks, and report them for resolution as part of the weekly status updates and the MSRs.

6.1.6 Government-Furnished Equipment

As facilities allow, contractor employees with access to the government facility and network access may be furnished the following equipment/access in support of this contract:

- Laptops.
- Mobile phones.
- Workspace with a workstation, telephone, and access to photocopiers, printers, and scanners for individuals assigned to work from a government facility. There is no guarantee that on-site government space will be available for support personnel on a daily basis.

The government shall provide the contractors, as appropriate, with access to the networks required to perform work on this contract. The Contractor will accomplish training and meet requirements to comply with and maintain DHS/CISA network access (see 9.15 DHS Information Security Policy).

The contractor shall retain, maintain, and deliver an asset inventory of Government Furnished Equipment (GFE) including hardware and software.

6.1.7 Contractor-Provided Equipment: Personal Protective Equipment and other Protective Supplies

Personal protective equipment (PPE) is designed to protect employees from serious workplace injuries or illnesses resulting from contact with biological, chemical, radiological, physical, electrical, mechanical, or other workplace hazards. Besides face shields, safety glasses, hard hats, and safety shoes, PPE encompasses a variety of devices and garments including the following:

- NIOSH approved respirators (all types and manufacturers)
- Nitrile gloves
- Hand Sanitizer
- Disposable garments
- Splash goggles (or other eye protection)
- Face masks
- Antimicrobial Soap
- Powered Air-Purifying Respirator with Full Face piece and High-Efficiency Particulate Air (HEPA) Filters
- Disposable Protective Clothing with Integral Hood and Booties
- Gowns
- Aprons

Appendix B of 29 CFR 1920.120 outlines in detail PPE requirements for emergency response and identifies three categories of PPE:

- Level A, used when the greatest level of skin, respiratory, and eye protection is required;
- Level B, used when the highest level of respiratory protection is necessary, but a lesser level of skin protection is needed; and
- Level C, used when the concentration(s) and type(s) of airborne substance(s) is known and the criteria for using air purifying respirators are met.

Level C is the most likely PPE level of protection expected to be needed by DHS contractors. The contractor will be required to supply its staff with the appropriate PPE, if necessary, to meet the SOW task requirements.

6.1.8 Contract Transition and Closeout

Upon contract award, the contractor shall work with the incumbent contractor to transition existing work from the incumbent. As this contract ends, the contractor shall develop a transition-out plan due ninety (90) calendar days prior to the end of the contract that shall be used to allow the current contractor to complete existing work and to transition ongoing work over to the new contractor.

Finally, the contractor will be required to complete a contract closeout to ensure finances, deliverables, and government property are appropriately handled.

The contractor shall work with the government and the incumbent contractor to follow their contract's transition out plan. The contractor shall proceed with accepting transitioned tasks in a manner that is most in-line with no disruption to mission and performance. A Transition In plan that corresponds to the incumbents Transition Out plan may be required.

The contractor shall develop and submit an outgoing 90-Day Transition Plan, transitioning work from the contractor to a successor contractor or Government entity. This transition may be to a government entity, another contractor, or to the incumbent contractor under a new contract. In accordance with the government-approved plan, the contractor shall assist the government in planning and implementing a complete transition from this contract to a successor contractor. This shall include formal coordination with government staff, and successor contractor staff and management. A Draft 90-Day Transition Plan shall be delivered to the government one-hundred and forty-five (145) calendar days prior to the end of the period of performance for government comment. A Final 90-Day Transition Plan delivered to the government one-hundred and twenty (120) calendar days prior to the end of the period of performance.

The 90-Day Transition Plan shall also include delivery of existing policies and procedures, security artifacts, and documentation. The 90-Day Transition Plan shall be tailored to the government requirements and address work functions and products that require transition to a new contractor, such as:

- Transition of historical data to the successor contractor's system(s).
- Transition of government approved contractor training materials and certification process documentation.
- Transfer of necessary business and/or technical documentation.
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates, and patches.
- Transfer of GFE and GFI to the government.
- Facilitation of applicable government debriefings and personnel out-processing procedures.
- Turn-in of all government keys, identification and access cards, and security codes.

Upon contract closeout, the contractor shall submit a closeout report to the government no later than ninety (90) calendar days before the contract period of performance (POP) completion date. The report should include, as a minimum, the following information:

- Financial Data - Breakdown of all costs (labor, travel, material, fee, and ODC) by contract line item number (CLIN) and sub-CLIN as applicable; all key personnel that were utilized/charged on the job; all work yet to be charged; all remaining funds; and balances available, if any, for return (de-obligation), etc.
- Deliverable Status – Percentage job complete, any outstanding issues, deliverable status,

list of any items/services under workmanship/manufacturer warranty, etc.

- Government Property – All Contractor-Acquired Property (CAP) and GFE provided for contract performance shall be accountable at the completion of each contract period. Property shall be consumed, transferred to an active contract, disposed of, or returned to the government at contract/TO closeout. Upon contract closeout, the contractor shall submit a final contract inventory list to account for all government property. For property being returned, the contractor must include on the inventory list the following minimum information: part numbers, National Stock Number (NSN) (if applicable), quantity, and condition of each item.

6.2 TASK 2: Operational Planning

The Contractor will support all aspects of CISA's operational planning efforts including planning that supports cyber defense operations, cyber incident response, incident response to natural disasters and terrorist attacks. Based on intelligence, knowledge about threats and vulnerabilities the contractor will develop realistic planning scenarios to support planning objectives. The contractor may participate in interagency campaign planning efforts to apply whole-of-government capabilities to defend and security our nation's infrastructure. Planning efforts may include but are not limited to:

- Development of contingency plans to respond to and recover from impacts to National Critical Functions
- Cyber defense operational plans
- Incident management plans
- Incident coordination plans
- Threat specific playbooks (ransomware, State and local cyber incident response, etc.)
- Campaign plans

The above plans will be developed to respond and recover from natural disasters such as hurricanes, wildfires, and pandemics as well as threat-based attacks (cyber and/or terrorism from criminals and/or national state actors).

The contractor will leverage the National Response Framework, National Incident Management System, and National Cyber Incident Response Plan.

The contractor will participate with and conduct joint planning with interagency, state and local, private sector and international partners.

The contractor shall write, edit, and publish planning documents in accordance with CISA standards and templates as well as providing graphic designs to enhance planning products. Additionally, the contractor can provide recommendations for improvements to documentation and writing processes and standards, as well as produce reports, briefings, talking points or other products in support of IOD as required.

6.2.1 Other Planning Products

In addition to the planning products outlined above IOD has the requirement to coordinate, develop, update, and deliver a number of other products including CONOPS, checklists to support plans, SOPs, Corrective Action Plans (CAPs), After-Action Reports (AARs), and others when directed by leadership. The contractor shall deliver the following products including, but not limited to:

- SOPs in support of steady-state CISA operations, processes, or procedures that ensure the efficient and effective use of CISA resources in accomplishment of its mission and to ensuring dissemination of critical information and assistance when identified threats to CISA missions/equities are identified.
- Checklists supporting CISA operations and plans from steady-state through all phases of incident response to focus resources thus ensuring expedited response, minimizing confusion, eliminating duplication of effort, ensuring communications, and reducing ambiguity.
- CAP and AARs will evaluate training and exercises to identify lessons learned, best practices, and areas for improvement. These evaluations support CISA's continuous improvement endeavors to revise plans, build and sustain capabilities, and maintain readiness by using Homeland Security Exercise and Evaluation Program (HSEEP) fundamental principles for exercise programs.
- Other plans/products may be required to be produced which leadership determines necessary.

6.2.2 Coordination

The contractor shall support IOD by effectively communicating and coordinating, as required, with the appropriate CISA elements in order to provide a more complete picture to IOD leadership regarding planning efforts or situations with leadership visibility.

6.2.3 Operations Support

The contractor shall be prepared to provide planning in direct support of ongoing operations. IOD provides operational planning and research, coordination and communication, data collection and analysis, as well as status updates, and oral and/or written reports to IOD leadership as directed.

6.3 TASK 3: Coordinate reviews of National, CISA, and IOD level plans

IOD must review, coordinate, and update numerous plans at various levels of the government and CISA/IOD. The various plans must be assessed to be sure they reflect current mission requirements, organizational equities, and complement, not contradict each other. Contractor support for this task requires Secret clearance and the associated DHS fitness.

6.3.1 The contractor shall assess National, CISA, and IOD-level plans as directed. Reviews include evaluating plans for CISA/IOD equities and identifying action items that must be accomplished to ensure CISA plans reflect higher headquarters intent and mission assignments.

6.3.2 The contractor shall produce and present planning products based on research and analysis of National level plans such as the National Response Framework, National Infrastructure Protection Plan, National Cyber Incident Response Plan, and National Incident Management System, particularly in regard to the CISA annexes to such plans. Contractor will develop specific CISA annexes/appendices to include in national-level planning documents.

6.4 TASK 4: Readiness (Training and Exercises)

The training and exercises program manages the functional areas of preparedness, planning, coordination, conduct, and evaluation for training and exercises, along with analyses and assessments focused on building preparedness and readiness and creating defendable and repeatable standards for measuring operational readiness for CISA. The training and exercises program establishes procedures to produce a continuous, integrated assessments of CISA's preparedness through each phase of the training and exercise development cycle. The training and exercises program ensures CISA regions, divisions and offices conducting training and exercises have appropriate guidance and tools to consistently analyze how their activities support CISA's continuous improvement endeavors to revise plans, build and sustain capabilities, support professional development, maintain preparedness, and an optimized and empowered workforce. This training and exercises program function establishes the means for developing and continuous improvement of personnel skills and core competencies to better meet the needs of CISA missions by common, continuous training and cross training coupled with rotational assignments, recognition programs, transparency. The contractor shall write, edit, and publish doctrine, policy directives, exercise, and training plans reflected in exercise plans, and lead/publish exercise AARs. The contractor shall apply knowledge of effective writing principles and practices executing day-to-day functional activities applying IOD processes, procedures, work instructions, and checklists, to develop and refine the IOD Suite of Training and Exercise Plans in accordance with the CISA style guide and the CISA/SPP Policy and Governance Frameworks. The contractor staff supporting this task must have a Top Secret/SCI/Secret clearance with the associated DHS fitness, depending on the position.

6.5 TASK 5: Surge Support (Optional)

Surge Support includes Tasks 2 for the rapid development of courses of action to support incident response, cyber defense operations and recovery. Additional contract staff to support these efforts must have prior approval of the COR. Surge support is not intended to perform steady state operations.

If surge support is required, the government shall identify the need and coordinate with the contractor for support to meet the new requirement.

6.6 TASK 6: Regional Planning Support (Optional)

The Contractor shall perform all tasks associated with TASK 2 above in direct support to Regional Director operational planning requirements and objectives. The contractor shall support the ten (10) Regions by driving the creation of a documentation methodology and framework, and maintain consistency and efficiency conducting research as required.

7.0 DELIVERABLES, MEETINGS, AND OTHER REPORTING REQUIREMENTS

Deliverable/Event	SOW Reference	Description	Due Date	Update Frequency
Kick Off Meeting	6.1.1	Briefing to discuss the minimum for TO completion: strategy for meeting contract requirements, presenting pertinent schedule and risk data, and key personnel introductions	Electronic draft 2 business days before the schedule briefing 10 copies of the kickoff briefing to the meeting	N/A
Monthly Status Report	6.1.2	MSR contains: • Staffing roster • Deliverable progress Deliverable issues Issues/Recommendations Schedule Performance Costs (estimated vs. actual) • Risks • GFE inventory	15 calendar days following the end of the previous calendar month	
Staffing Plan	6.1.3.1	Staffing roster contains: • Labor category descriptions/qualifications proposed • Percentage of personnel currently available by labor category by applicable task • Percentage of personnel currently available by labor category with TS/SCI personnel security clearances • Proposed approach for supporting surge requirements	First Draft due with Proposal Final draft due 45 days after contract award	Updated each month in the monthly status report.
(a) Weekly and Ad hoc Meetings	All Tasks	Contractor to provide meeting minutes	(a) Weekly *- and -*	As needed

Deliverable/Event	SOW Reference	Description	Due Date	Update Frequency
- and - (b) Meeting Minutes/Actions			(b) As soon as possible but no later than 2 days after meeting	
Program Management Review (PMR)	6.1.2	Monthly PMR meeting with government. PMR Report will include: • Contract Financial Status • Contract Performance metrics • Mitigation plan for under-performing areas • Status of other risks, issues, problems, and concerns and proposed solutions	48 hours before scheduled PMR	Monthly
Transition In Plan	6.1.8	The contractor shall work with the government and the incumbent contractor to follow their contract's transition out plan. The contractor shall proceed with accepting transitioned tasks in a manner that is most in-line with no disruption to mission and performance. A Transition In plan that corresponds to the incumbents Transition Out plan may be required.	As Required	As needed
Transition Out 90 Day Plan	6.1.3	Includes delivery of existing policies and procedures, security artifacts, and documentation tailored to the government requirements and may include, but is not be limited to: • Coordination with government representatives. • Review, evaluation, and transition of current contractor		

Deliverable/Event	SOW Reference	Description	Due Date	Update Frequency
		support services. • Transition of historical data to the successor contractor's system(s). • Transition of government approved contractor training materials and certification process documentation. • Transfer of all necessary business and/or technical documentation. • Transfer of compiled and un-compiled source code, to include all versions, maintenance updates, and patches. • Transfer of GFE and GFI to the successor contractor. • Transfer of the GFE inventory management system, all user and maintenance documentation, and current GFE information in the system to the successor contractor. • Facilitation of applicable government debriefings and personnel out-processing procedures. • Turn-in of all government keys, identification and access cards, and security codes.	Draft 90-Day Transition Plan due 145 days prior to the end of POP. Final 90-Day Transition Plan due 120 days prior to the end of POP	As needed
Contract Closeout	6.1.3	Contract closeout and transition out reports including the following information: • Financial data • Deliverable status • Government Property	Due 90 days before the contract POP completion date	N/A
Staff Actions, CONOPS, Plans,	Task 2	Produce reports, briefings,	As	As needed/Government

Deliverable/Event	SOW Reference	Description	Due Date	Update Frequency
SOPS, AARs, CAPs, Checklists, Other Products		talking points, CONOPS, Plans, SOPs, AARs, CAPs, or other products in support of IOD/Subdivisions	needed/Government request	request
National Level Plan Support Documents	6.3.2	Specific CISA annexes/appendices to national level planning documents.	As needed/Government request	As needed/Government request

*Unless otherwise noted, all days are calendar days

All deliverables will become the property of the government. Any informal or formal deliverables shall be provided in CISA-approved formatting with no additional contractor labels or contractor clauses. All work performed, all deliverables, all products, all approaches will become the sole property of the United States Government.

8.0 CONTRACT PERFORMANCE

8.1 Place of Performance

Due to limited office space, the primary place of performance will be remote. Remote work includes contractor personnel working at the contractor's facility or teleworking at their personal residences. Government on-site rates shall be charged when contractor personnel are teleworking at their personal residences. All personnel are expected to reside within National Capital Region (NCR) and are required to routinely commute to government facilities within the NCR for meetings and classified work. The Government reserves the right to revoke telework privileges and require contractor personnel to come into government facilities on a regular basis when deemed necessary to meet the requirements stated within the SOW. Local travel within a 50-mile radius of the NCR or the contractor facility will not be reimbursed. Work may be performed at the following government locations:

- Staff support site:
    - Glebe Road Facility (Ballston II) 1110 N. Glebe Road Arlington, VA;
    - DHS HQ at St. Elizabeth's Campus 2700 Martin Luther King Jr. Avenue SE, Washington, DC 20528
    - Corry Station, 1000 Chiefs, BLDG 3782 Way Pensacola, FL
    - Optional Tasks – 10 regional office headquarters
- Continuity Facilities: MWEOC19844 Blue Ridge Mountain Road, Bluemont, VA 20135
- Temporary work locations may be designated at other federal government sites within the National Capitol Region, as well as the CISA Continuity of Operations (COOP)

location to include, FEMA HQ – 500 C Street SW, Washington, DC 20024

- For most SOW tasks or functions within a task, the contractor may propose contractor facilities. If the contractor chooses to do this, the contractor shall make that clear in the Staffing Plan submitted with their proposal. There is no guarantee that on-site government space will be available for support personnel on a daily basis. DHS SCIF space is available for classified work.

8.2 Period of Performance

The period of performance for this task order is a one-year base period with three (3) one-year option periods as follows.

Anticipated Performance Period	Performance Period Dates
Base Period	12/15/2021 – 12/14/2022
Option Period 1	12/15/2022 – 12/14/2023
Option Period 2	12/15/2023 – 12/14/2024
Option Period 3	12/15/2024 – 12/14/2025

8.3 Contractor Personnel

The PM will be the contractor's authorized representative for the technical and administrative performance of all services required under this Task Order. The PM will serve as the first POC for Task Order or administrative questions or difficulties that arise related to this Task Order. The PM will be the primary point through which communications, work assignments, and technical direction flow between the Government and the Contractor.

The PM or designated alternate will be available during normal work hours to meet with DHS, in person or as otherwise agreed upon by DHS, to discuss problem areas. In the event of disaster recovery or COOP events, the PM will be available during normal hours of operation, and during periods of no-notice emergencies, including localized acts of nature, accidents, and military or terrorist attacks. The PM will provide the necessary level of contract management and administrative oversight to achieve the quantitative and qualitative requirements of the contract. The PM or alternate shall also have full authority to act for the contractor on all matters relating to daily operation of this Task Order.

The contractor shall ensure that employees are competent in operational planning processes and functions, critical thinking, research and analysis, technical writing and editing and will strive to include industry best practices in the respective fields of functional expertise.

8.3.1 Covered Hours for Core Work

Standard covered business hours are 7:00 a.m. to 5:00 p.m. Monday through Friday. Personnel are expected to have work coverage during these hours and are expected to work eight hours per

day (M-F).

8.3.2 Hours for Surge Work

Surge support may require extended hours beyond the normal CORE non-shift hours.

8.4 Travel

The Contractor may be required to travel to other CISA locations. All travel must be in accordance with the Federal Travel Regulation and FAR 31.205-46. Where possible and when deemed effective, the contractor will employ collaborative services and technologies such as email, chat applications, telephone bridges, and video and web conferencing as economical alternatives to travel. When travel is necessary, the contractor will adhere to the following requirements:

1) The contractor will submit a Travel Authorization Request to the PERT COR that specifies travel dates, expected duration, origin and destination, purpose, estimated costs, and the number and names of personnel traveling. The PERT COR must provide written approval of the Travel Authorization Request before the contractor is authorized to incur any travel expenses.
2) Reimbursement for travel will be in accordance with FAR Part 31.205-46. Travel compensation will not exceed the government allowance for travel and per diem. The COR will certify invoices prior to processing for payment.

8.5 Other Direct Costs (ODC's)

Prior approval by the COR is required for any ODC. The contractor will provide three (3) quotes and justification for the purchase with its approval request. All equipment must be in compliance with the Buy American Act and Trade Agreements Act. Allowable and reasonable costs incurred by the contractor for other direct costs will be reimbursed. Section 12.0 provides a detailed list of all documents that must be included when invoicing for an ODC; failure to comply with these requirements will result in a rejected invoice.

8.6 Identification of Non-Disclosure Requirements

Some material will contain proprietary, sensitive, or classified data from various public or private sources. The Contractor must require all subcontractors to sign corporate and individual non-disclosure agreements (NDAs).

8.7 Enhanced Skills Training

The government will not pay for contractor training required to perform work under this contract. For training that provides direct benefit to the work being performed by the contractor under a specific task, the contractor may request the government approve attendance

on a case-by-case basis. In the event the government does not approve the contractor's ODC request for tuition, per diem, and/or travel costs, but approves the training, the contractor shall submit a request to bill the government only for the labor hours to attend training. The COR will review all requests and approve or disapprove on a case-by-case basis.

8.8 Accessibility Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this SOW must comply with the applicable technical and functional performance criteria of Section 508 unless exempt.

8.8.1 Section 508 Applicable Exceptions

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 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.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

   Item that contains Information and Communications Technology (ICT): security assessment reports

   Applicable Exception: National Security **Authorization #:** NPPD 20110202-001

2. 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 January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

DHS Office of Accessible Systems and Technology has reviewed this acquisition request and has determined that a "National Security Exception" for the purposes of Section 508 applies and is thereby authorized. National Security Exception # NPPD 20110202-001 approved on February 2011 was approved on the C-LAN network and cannot be attached to this SOW.

8.9 Audit Rights

The contractor will allow DHS access to contractor facilities to audit performance under the contract.

9.0 SECURITY REQUIREMENTS

Any work performed at Government facilities is subject to DHS security requirements.

The following security requirements are applicable under this SOW:

DHS 4300A Policy 1.5.1.a: This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

DHS 4300A Policy 4.1.2.a: Components will ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.

DHS 4300A Policy 4.1.2.b: Components will ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.

DHS 4300A Policy 3.3.a: All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.

DHS 4300A Policy 3.3.b: Contractor information system services and operations shall adhere to all applicable DHS information security policies.

DHS 4300A Policy 3.3.c: Requirements will address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements must also include conditions for personnel background investigations and clearances and facility security.

DHS 4300A Policy 3.3.d: SOWs and contracts will include a provision stating that, when the

contract ends, the contractor will return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system(s) that have been used to process DHS information.

DHS 4300A Policy 3.3.e: Components will conduct reviews to ensure that information security requirements and provisions to address supply chain risk are included in contract language and that the requirements and provisions are met throughout the life of the contract.

DHS 4300A Policy 3.3.f: Security deficiencies in any outsourced operation require creation of a program-level POA&M.

DHS 4300A Policy 3.3.g: Components must require contractors to apply information system security engineering principles in the specification, design, development, implementation, and modification of information systems, in accordance with NIST Special Publication (SP) 800-27, Engineering Principles for Information Technology Security.

DHS 4300A Policy 3.3.i: For systems with high or moderate impact for any of the FIPS 199 security objectives, components will require developer of information systems, system components, or information system services to:

1. Create and implement a security assessment plan
2. Perform unit, integration, system, regression testing/evaluation commensurate with the volume and complexity of modifications and the impact to the system risk made by those modifications
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation
4. Implement a verifiable flaw remediation process
5. Correct flaws identified during security testing/evaluation.

DHS 4300A Policy 3.3.j: All SOWs, contract vehicles, and other acquisition-related documents must include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and SPs.

DHS 4300A Policy 4.3.1.a: Components will ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as Universal Serial Bus (USB) drives, are stored when not in use in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons).

DHS 4300A Policy 4.3.1.c: DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-government-issued removable media (such as USB drives) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.

DHS 4300A Policy 4.3.1.e: DHS-owned removable media must not be connected to any non-

DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). The respective CISO is the CISO with that system in his or her inventory.

DHS 4300A Policy 4.1.5.b: DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) accessing DHS systems must receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness training within 24 hours of being granted a user account. If a user fails to meet this training requirement, user access will be suspended.

DHS 4300A Policy 4.1.5.c: DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) will receive initial specialized training and thereafter annual refresher training specific to their security responsibilities.

9.1 General

The DHS Office of the Chief Security Officer (OCSO) has primary security cognizance of all SCI work performed during the performance of this contract and subsequent contract phase unless otherwise directed by the government.

All contractor personnel assigned to those tasks specifically noted as requiring a Top Secret clearance must be U.S. Citizens and meet the requirements contained in DHS Directive 121-01-007, Personnel Fitness and Security Program. All contractor employees must complete the DoD Information Assurance Awareness, Web Based Training (WBT), dated September 2001, version 1.0 or higher, as a minimum training requirement. All contractor employees are subject to the training requirements listed in Section 9 Information Technology Security and Privacy Training. The contractor must track completion of this required training and inform the government

DSS has realigned to DCSA approximately two years ago. Contract identifies that security requirements range from TS/SCI to Public Trust. Based upon this information the company awarded the contract must possess a TS FCL to support the highest level of clearance and access level.Contractor's request for visit authorization to the government facility located at the in Arlington, VA shall be submitted in accordance with the appropriate facility visitor policy. Contractors requests for visit authorization to the Government facility located in Pensacola, FL shall be submitted in accordance with the Corry Station facility visitor policy. Upon request, a copy of each policy will be provided.

The government reserves the right to approve or deny fitness of the contractor's individual employees based on security risks, unsatisfactory performance, or disruptive influence to mission accomplishment.

While the DHS contractor fitness process averages 120 days from submission to date of EOD, the timeline can vary significantly (90 days to 180 days) based on an individual's clearance status and

whether or not they have exceptions tied to their clearance. Therefore, the contractor should plan for the DHS contractor fitness process to take 90-180 days from the date of required documentation submission to the date of EOD approval notification from DHS. After receiving DHS EOD approval for contractor staff, the contractor should plan for a 30-day timeframe to obtain government furnished equipment, including laptops, cell phones, and elevator cards. DHS will work with the contractor to make the turn-around time for both fitness and equipment as efficient as possible.

9.2 Sensitive Compartmented Information (SCI) Elements

The Contractor is required to hold and maintain a Top Secret Facility Clearance Level (FCL). The contractor's personnel will be required to hold and maintain Top Secret clearances with access to SCI to perform the requirements under this SOW. The contractor's personnel will be required to access TS/SCI data throughout the period of performance.

All employees performing work with an SCI delegation are allowed to perform work within a government or government-sponsored SCIF. Additionally, the contractor must already have access to SCIF space where they can perform the work.

9.3 Access to and Protection of Classified Information

The Contractor will ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

Performance on this contract requires the contractor to gain access to classified National Security Information (includes documents and material), which mandates protection in accordance with Executive Order 13526 National Security Information (NSI), as amended, as well as any supplemental directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification (an attachment in the task order), the National Industrial Security Program Operating Manual (NISPOM), as well as any relevant Intelligence Community Directives (ICDs) for protection of classified and/or compartmented information at its cleared facility, if applicable, or as further directed by the Special Security Officer (SSO)/Office of Selective Acquisition Security Manager (OSASM). If the contractor requires access to classified information at any DHS or other government facility, they will abide by the security requirements set forth by the Cognizant Security Authority (CSA) for that facility.

The DHS Office of the Chief Security Officer (OCSO) has primary security cognizance of all SCI work performed during the performance of this contract and subsequent contract phase unless otherwise directed by the government.

DHS will inspect all SCI Facilities accredited by DHS and all material generated or processed under the purview of this contract. All SCI will be handled in accordance with special security requirements, which will be furnished by the responsible SSO/OSASM.

The contractor shall ensure these instructions are expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

9.4 Personnel Security (PERSEC) and Contractor Fitness Requirements

All contractor personnel assigned to this contract must be U.S. Citizens and meet the requirements contained in DHS Instruction 121-01-007, Personnel Fitness and Security Program.

All contractor personnel assigned to this contract shall possess security clearances commensurate with the level of required access to classified information that is directly in support of this contract. Contractors are responsible for providing personnel with the required security clearances as DHS does not sponsor security clearances for contractor personnel. Additionally, non-U.S. citizens, personnel cleared on an interim basis, or personnel holding contractor-generated Confidential clearances are not eligible for access to sensitive or classified information released or generated under this contract.

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 fitness.

Contractor personnel who are specifically designated as requiring access to SCI must be eligible under the provisions of the ICD 704 without exception.

Requests for Access (RFAs) will be submitted by the government project manager who will validate the justification for access. Once validated, the request for access will be verified by the COR and approved by the OSA SM/SSO for the process of SCI. If approved for SCI access, contractor personnel must be indoctrinated by a DHS SSO prior to being granted access to SCI information. All PERSEC reporting requirements as outlined in ICD 704 will be made directly to the responsible SSO.

Upon Contract Award, the contractor shall fill out and submit DHS form 11000-25 Contractor Fitness/Security Screening Request Form to the COR within seven (7) business days. Contractor employees (to include applicants, temporary, part-time, and replacement employees) under this contract who need access to sensitive information shall undergo a contractor fitness risk assessment determination based on the duties each individual will perform on the contract. All DHS contractor fitness determinations will be processed through the DHS Security Office. Unless an applicant requiring access to sensitive information has resided in the United States for three of the past five years, the government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

9.5 Background Investigations

Contractor employees (including temporary, part-time, and replacement employees) under this contract needing access to sensitive information will undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis should identify the appropriate background investigation to be conducted. All background investigations are processed through the DHS OCSO, Personnel Security Division. Unless an applicant requiring access to sensitive information has resided in the United States for three of the past five years, the government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

9.6 Required Documentation

Each contractor employee (including applicants, temporary, part-time and replacement employees) who requires access to classified information to perform their obligations under this contract must be U.S. citizens and have been granted a security clearance by the U.S. Government (Interim Top Secret clearances are not accepted by DHS). Prospective contractor employees should submit the following completed forms to DHS OCSO/PSD prior to entry on duty of any employee, whether a replacement employee, additional employee, subcontractor employee, or vendor:

- Standard Form (SF) 86C, "Standard Form 86 Certification"
- DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- Standard Form (SF) 85P, "Authorization for Release of Information"

Only complete packages will be accepted by the DHS OCSO. Specific instructions on submission of packages will be provided upon award of the contract.

9.6.1 Contractor Fitness Determinations

Contractor staff may provide limited support to the government while their contractor fitness packages are being processed by the government, with the understanding that the following restrictions listed below apply:

- The individual only has limited access to DHS facilities for transitional purposes once their contractor fitness packages have been submitted to PSD for processing.
- The individual must not access DHS classified information regardless of their current clearance status without an EOD contractor fitness decision from PSD.
- The individual must not access to any DHS accounts (A-LAN, MOE, etc.).
- The individual will not be granted any GFE (i.e. computer, datawatch card etc.).
- The individual will only have access to unclassified information.

- The individual will not have access to sensitive unclassified information nor FOUO information as per DHS directive 121-0l-007.
- The individual must be escorted by a government employee.

The granting of a favorable EOD decision is not be considered as assurance that a final contractor fitness determination will follow. A favorable EOD decision or a final contractor fitness determination in no way prevents, precludes, or bars DHS from withdrawing or terminating access to facilities or information at any time during the term of the contract. No employee of the contractor is allowed unescorted access to a government facility without a favorable EOD decision or final contractor fitness determination by the OCSO.

All DHS contractor fitness determinations will be processed through DHS OCSO.

9.7 Continued Eligibility

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

9.8 Termination

The Contractor will notify the SSO/OSASM and COR of all terminations/resignations of contractor personnel assigned to this contract ten (10) working days before the last day of employment. In the event this notification is not possible, the SSO/OSASM and COR should be notified immediately. The contractor will return all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees to the SSO/OSASM. If an identification card or building pass is not available to be returned, a report must be submitted to the SSO/OSASM and COR, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

9.9 Information Technology (IT) Security Requirements

When sensitive government information is processed on DHS telecommunications and automated information systems, the contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS IT Security Program Publication DHS MD 4300. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with DHS 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).

The Contractor shall configure its computers that contain DHS data with the applicable United States Government Configuration Baseline (USGCB) and ensure that its computers have and maintain the latest operating system patch level and anti-virus software level. (Note: USGCB is applicable to all computing systems using Windows 10 and later including desktops and laptops—regardless of function—but not including servers.)

9.10 Citizen Requirements for IT Contracts

Non-US citizens shall not be authorized to access or assist in the development, operations, 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 CIO or their designees. Within DHS HQ, 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:

- The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
- There must be a *compelling* reason for using this individual as opposed to a U.S. citizen; and,
- The waiver must be in the best interest of the Government.

9.11 IT Security Training and Oversight

Before receiving access to IT resources under this contract, the individual must receive a security briefing and complete any nondisclosure agreement(s) furnished by DHS.

9.12 Security Review

The government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced.

9.13 Access to Unclassified Facilities, IT Resources, and Sensitive Information

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors must comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures for all task orders that require access to DHS facilities, IT resources, or sensitive information. Contractors must not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

Contractor access to information protected under the Privacy Act is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

The parties agree to implement Title 6 Code of Federal Regulations Section 29.8(c) to govern procedures for handling critical infrastructure information. The regulations detailed in the 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 CII without a prior written certification from the Protected CII Program Manager or a Protected CII Officer that conforms to the requirements of Section 29.8(c) of the regulations in the Rule.

The Contractor shall comply with all requirements of the Protected CII (PCII) Program set out in the CII Act, in the implementing regulations published in the Rule, and in the PCII Procedures Manual as they may be amended from time to time and shall safeguard Protected CII 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. The Contractor shall ensure that each of its employees, consultants and subcontractors has executed a NDA and agrees that none of its employees, consultants or sub-contractors will be given access to Protected CII without having previously executed a NDA.

9.14 Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems should be established only through controlled interfaces and via approved service providers. The controlled interfaces must be accredited at the highest security level of information on the network. Connections with other federal agencies should be documented based on interagency agreements: Memorandum of Understanding (MOUs), Service Level Agreements (SLAs), or Interconnections Security Agreements (ISAs).

9.15 DHS Information Security Policy

All services provided under this task order must be compliant with DHS Information Security Policy, identified in:

- DHS Directive 4300, Information Technology Systems Security
- DHS MD 140-1 (formerly 4300.1), Information Technology Systems Security Program
- DHS MD 4300A Sensitive Systems Handbook
- DHS National Security System Policy 4300B
- DHS Sensitive Compartmented Information (SCI) Systems Policy 4300C

- DHS Systems Engineering Life Cycle (SELC) Guide
- Other Department of Homeland Security (DHS) Policy
- Committee for National Security Systems (CNSS)
- National Institute for Standards and Technology (NIST) Special Publications
- Other compliance bodies as identified by the government
- NCPS Continuous Monitoring

9.16 Security Requirements for Cryptographic Modules

The Contractor shall use Federal Information Processing Standard (FIPS) 140-2 compliant encryption (Security Requirements for Cryptographic Module, as amended) to protect all instances of DHS sensitive information during storage and transmission. The contractor shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (see https://csrc.nist.gov/publications/fips) to confirm compliance with FIPS 140-2 (as amended). The Contractor shall provide a written copy of the validation documentation to the Contracting Officer and the Contracting Officer's Technical Representative.

The Contractor shall ensure that this standard is incorporated into the Contractor's property management/control system or establish a separate procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive DHS information. The Contractor shall ensure that its subcontractors (at all tiers), which perform work under this contract comply with the requirements contained in this clause.

9.17 Advanced Encryption Standard

The Contractor should use cryptographic protection of DHS sensitive (unclassified) information, as defined in P. L. 100-235, and must comply with FIPS PUB 197 (as amended).

9.18 DHS Security POC/SSO/OSASM

Department of Homeland Security
Office of the Chief Security Officer
Special Security Programs Division
[redacted]

10.0 ACCOUNTABLE PROPERTY

Definitions:

- Accountable Personal Property - An asset that meets one or more of the following criteria: (1) expected useful life is two years or longer and an asset value and/or acquisition cost of $5,000 or more; (2) that is classified as sensitive; (3) for which

accountability or property control records are maintained; (4) Capitalized personal property, (5) Leased property that meets accountability standards, or (6) otherwise warrants tracking in the property system of record. Current accountable personal property information may be obtained through the CS&C APO Office at [redacted]

- Capitalized Personal Property - Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Current Capitalization Threshold information may be obtained through the CS&C APO Office at [redacted]
- Contract Property - Contract property refers to both Contractor-Acquired Property (CAP) and GFP, in the possession of contractors.
- Contractor Acquired Property (CAP) - Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.
- Government Furnished Property (GFP) - Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as Government Furnished Equipment (GFE), the two terms are interchangeable.
- Leased Property - Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).
- Sensitive Personal Property - All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse; national security or export control considerations. Such property includes but is not limited to, weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. Current sensitive personal property information may be obtained through the CS&C APO Office at [redacted]

Property Accountability:

- When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property
- It is the contractor's responsibility to use contract property as it was authorized, and for the purpose intended. In the event the contractor uses contract property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs
  Contractor is directly responsible and accountable for all contract property in its possession in accordance with the requirements of the particular contract; this also includes any contract property in the possession or control of a subcontractor

Physical inventory: In addition to requirements provided under the contract's government property clause:

- The Contractor shall, minimum annually, perform, record, and disclose physical inventory results of CAP and GFP to the CS&C APO Office at [redacted] PA and/or COR
- Annual inventory results will be completed, certified and submitted by close of business 31 May each year to the CS&C APO Office at [redacted] PA and/or COR
- The Contractor shall, upon request, perform, record, and disclose physical inventory results of CAP and GFP to the CS&C APO Office [redacted] PA and/or COR
- As requested inventory results will be completed, certified and submitted, in the timeframe defined at the time of request, to the CS&C APO Office at [redacted] PA and/or COR

Property Disposal:

- All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable government rules and regulations for disposal of government property. Further, the contractor shall provide necessary information to the PA, COR and the CS&C APO Office at [redacted]. For all excess property prior to taking any action. Excess personal property" means any personal property under the control of a Federal agency that the agency head determines is not required for its needs or for the discharge of its responsibilities.

Lost, Stolen, Damaged or Destroyed (LDD) property:

- Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear in accordance with the contract's government property clause.
- Any occurrence of LDD must be investigated and fully documented by the PA and/or COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the PA in accordance with the contract's government property clause and as detailed below, as soon as it becomes known
- When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from CS&C APO Office at [redacted]
- A Report of Survey will be prepared, regardless whether or not preliminary research of a LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.
- The Contractor must forward this document with all supporting documentation to the PA or COR within 5 business days of the LDD event for review.

- The PA and/or COR must submit the completed package to [redacted] within 5 business days of receipt from the Contractor.
- Contractor, PA and/or COR must supply all requested information and any subsequent requests for information.

11.0 INVOICES

Deliverables: The Contractor shall provide invoices for all Accountable Personal Property within 30 days of acquisition to the Property Administrator (PA) and COR.

Invoices:

- All invoices shall contain the CLIN and Accounting Classifications, contract number, purchase order number, Supplier's name, Supplier's phone number, manufacturer, manufacturer part number, manufacturer model number, serial number, quantities, item descriptions, and unit cost.
- The purchase order number shall be on all invoices, packages, bills of lading, correspondence, and any other documents pertaining to the contract.
- Separate invoices are required for each purchase order.

All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and ENERGY Star standards. Scope qualifies for DHS CATEX A5 and B3. These CATEXs should be noted in the project file and also stated in future ITAR submission in support of this contract.

12.0 MATERIALS/OTHER DIRECT COSTS (ODC)

ODC CLINs will be separated for IT and NON-IT requests. Materials/ODCs include but are not limited to computer service center costs, Training, Exercise, and Planning supplies and specialized requirements, document reproduction costs, equipment, supplies, shipping, and procurement (software and hardware) when essential to the task performance of this SOW. The contractor shall attain government approval in advance of incurring any costs associated with Other Direct Costs (ODCs). The Contracting Officer (CO) provides government approval when over $2,000.00 and Contracting Officer Representative (COR) may provide approval when under $2,000.00. All materials purchased by the contractor for the use of or on behalf of the government become the property of the government at the time of purchase. All purchase orders, contracts, and similar instruments shall contain language establishing that the purchaser of record for purposes of ownership and warranty is the Department of Homeland Security, National Communication Coordination Branch. The contractor shall require vendors to acknowledge this fact on the invoice, packing slip, warranty record, or other suitable documentation. If vendor does not comply, contractor shall provide a statement to the same effect, signed by a company official, within three business days of receipt of the purchased goods or services. The transfer of materials must be documented by the contractor; in addition to an accounting of all materials consumed, purchased or leased during the performance of individual elements of the contract. The contractor must

furnish the government a copy of such documents with the Monthly Status Reports. Materials to be delivered to DHS facilities shall be handled in accordance with DHS policies and procedures. DHS goods shall not be delivered to contractor offices or contractor personnel homes in order to circumvent DHS policies and procedures.

13.0 ENERGY STAR REQUIREMENTS

All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and ENERGY Star standards.

14.0 PRIVACY PROVISIONS

14.1 References:

DHS Management Directive 140-01, "Information Technology Security Program

DHS National Security Systems Policy Directive 4300A, Version 13.1, July 25, 2017

DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclassified, Secret or Top-Secret Collateral).

'DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017' for TS SCI/C-LAN.

15.0 SECURITY

Safeguarding of Sensitive Information (MAR 2015)

15.1 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.

15.2 Definitions. As used in this clause—

15.2.1 "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.

15.2.2 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.

15.2.3 "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:

15.2.3.1 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);

15.2.3.2 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);

15.2.3.3 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

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

15.2.4 "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.

15.2.5 "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:

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

15.2.6 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.

15.3 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:

- DHS Management Directive 11042.1 Safeguarding Sensitive but Unclassified (for Official Use Only) Information
- DHS Sensitive Systems Policy Directive 4300A
- DHS 4300A Sensitive Systems Handbook and Attachments
- DHS Security Authorization Process Guide
- DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Fitness and Security Program
- DHS Information Security Performance Plan (current fiscal year)
- DHS Privacy Incident Handling Guidance
- Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
- 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
- NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

15.4.1 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. DHS Sensitive Systems Policy Direction 4300A Version 13.1, July 27, 2017 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.

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

15.4.3 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.

15.4.4 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.

15.5 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.

15.5.1 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.

15.5.2 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.

15.5.3 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.

15.5.4 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.

15.5.5 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:

15.5.5.1 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

15.5.5.2 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.

15.5.6 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.

15.5.7 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.

15.5.8 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.

15.5.9 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.

15.6 Sensitive Information Incident Reporting Requirements.

15.6.1 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.

15.6.2 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:

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

15.7 Sensitive Information Incident Response Requirements.

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

15.7.2 The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all

requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

15.7.3 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.

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

15.8 Additional PII and/or SPII Notification Requirements.

15.8.1 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

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

- 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.

15.9 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:

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

15.9.2 Provide credit monitoring services to individuals whose data was under the control of the

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

- 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

15.9.3 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.

15.10 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.

16.0 INVOICE AND PAYMENT PROVISIONS

SINGLE PAYMENT OFFICE

The Contractor shall submit all invoices to [redacted] with copies to the Contracting Officer (CO), the Contract Specialist (CS), the Contracting Officer's Representative (COR), and the Alternate COR (ACOR). In order to facilitate the government's efforts to validate and approve the charges on the contractor's monthly invoice, the contractor shall provide detailed data supporting the charges on each invoice. The types of data required shall include, but is not limited to, the following:

LABOR

- Cover sheet identifying DHS;
- Task Order Number;
- DUNS Number;
- Month services provided;
- Employee roster with hours worked;
- Charge Code;
- Project name (if applicable);
- Program supported;
- Employee name;
- Company;
- Labor category;
- Hours worked;
- When was work performed

ODC's

- Purchase Order;
- Packing slips;
- Electronic delivery for software;
- Renewal confirmations;
- Project name (if applicable);
- Item type (Accountable/Unaccountable Hardware, Accountable/Unaccountable Software);
- Description;
- Serial Number, DHS Barcode (if known);
- Approved estimated cost;
- Actual cost

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.

17.0 ACRONYM LIST

A&A	Authorization and Assessment
AFS	Analytic Framework and Security
AMAC	Advanced Malware Analysis Center
ATO	Authority to Operate
BOE	Body of Evidence
BOM	Bill of Material
C&A	Certification & Accreditation
CAP	Contractor Acquired Property
CAGE	Commercial and Government Entity
CLIN	Contract Line Item Number
CM	Continuous Monitoring

CNCI	Comprehensive National Cybersecurity Initiative
CNSSI	Committee on National Security Systems Instructions
CNSSD	Committee on National Security Systems Directive
CO	Contracting Officer
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
CS&C	Cybersecurity and Communications
CSA	Cognizant Security Authority
CSP	Commercial Service Providers
CTO	Chief Technology Officer
DD	Department of Defense
DHS	Department of Homeland Security
DOD	Department of Defense
E3A	EINSTEIN 3 Accelerated
EAC	Estimates at Completion
ECS	Enhanced Cybersecurity Services
EIT	Electronic and Information Technology
EO	Executive Order
EOD	Entry on Duty
EPMO	Enterprise Performance Management Office
FCL	Facility Clearance Level
FEA	Federal Enterprise Architecture
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FNR	Federal Network Resilience
FOCI	Foreign Ownership and Control
FOUO	For Official Use Only
FSAM	Federal Segment Architecture Methodology
FSR	Financial Status Report
GFI	Government Furnished Information
GFP	Government Furnished Property
GOV	Government
HSPD	Homeland Security Presidential Directive
ICD	Intelligence Security Directive
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IG	Inspector General
IMS	Integrated Master Schedule
IOD	Integrated Operations Division
IPT	Integrated Product Team
ISA	Interconnections Security Agreement

ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information Security Vulnerability Management
IT	Information Technology
LOE	Level of Effort
MD	Management Directive
ME&T	Mission Engineering & Technology
MOA	Memorandums of Agreement
MOE	Mission Operating Environment
MOU	Memorandum of Understanding
MSR	Monthly Status Report
NCCIC	National Cybersecurity and Communications Integration Center
NCPS	National Cybersecurity Protection System
NCS	National Communications System
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NISPOM	National Industrial Security Program Operating Manual
NS/EP	National Security/Emergency Preparedness
NSD	Network Security Deployment
NSI	National Security Information
NSN	National Stock Number
NSPD	National Security Presidential Directive
OCI	Organizational Conflict of Interest
OCSO	Office of the Chief Security Officer
ODNI	Office of the Director of National Intelligence
ODC	Other Direct Cost
OE	Operations Environment
OP	Operational Plans Subdivision of IOD
ORC	Operational Readiness and Continuity Subdivision of IOD
OPSEC	Operations Security
OSASM	Office of Selective Acquisition Security Manager
PCAP	Packet Capture
PERSEC	Personnel Security
PM	Program Manager
PMO	Program Management Office
PMP	Project Management Plan
PMP	Project Management Professional
PMR	Program Management Review
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Period of Performance
R&D	Research and Development
RAR	Risk Assessment Report
RFA	Request for Access
RMF	Risk Management Framework

ROE	Rules of Engagement
S	Secret
SAP	Security Assessment Plan
SAR	Security Assessment Report
SAWP	Security Assessment Work Plan
SCA	Security Control Assessor
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCG	Security Classification Guide
SCM	Strategy Coordination and Management Office
SCRM	Supply Chain Risk Management
SCTMs	Security Controls Traceability Matrices
SE&I	Systems Engineering & Integration
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
SECONOP	Security Concept of Operations
SELC	System Engineering Life Cycle
SF	Standard Form
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLTT	State Local Tribal Territorial
SME	Subject Matter Expert
SMN	Security Management Network
SOP	Standard Operating Procedures
SOW	Statement of Work
SP	Special Publication
SRG	Security Requirements Guide
SSO	Special Security Officer
SSP	Security System Plan
STE	Secure Terminal Equipment
TS	Top Secret
T&E	Test & Evaluation
TTP	Tactics, Techniques, and Procedures
UARCs	University Affiliated Research Centers
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
WBS	Work Breakdown Structure