DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
Modeling Capability Transition Environment (MCTE) Support Services

August 2020

1.0 GENERAL
This Statement of Work (SOW) defines the technical services requirements necessary to support the Modeling Capability Transition Environment (MCTE) Application, hereinafter referred to as "APPLICATION". The APPLICATION is a secure web-enabled platform hosted in the FedRAMP-approved AWS GovCloud (US).

1.1 BACKGROUND
The National Risk Management Center (NRMC) develops analytic capabilities to support infrastructure consequence analysis to inform decisions by DHS and public and private sector partners. The NRMC analyses assist the Cybersecurity and Infrastructure Security Agency (CISA) in framing policy and programs, prioritizing its operational activities and maximizing operational effectiveness through more efficient use of resources.

The NRMC manages the National Infrastructure Simulation and Analysis Center (NISAC) to advance understanding of emerging risks across the cyber-physical domain. The NRMC represents an integration and enhancement of DHS's analytic capabilities, supporting stakeholders and interagency partners.

The APPLICATION provides NRMC with an accessible analytic environment where analysts can integrate, refine and execute analytical models, conduct simulations, and perform geospatial and calculated analyses in a risk analytics workflow system.

APPLICATION capabilities are delivered via four discrete environments:

1. Infrastructure – This environment provides the Dev/Ops tools and services for the development team. These tools include directory, email and GitLab Continuous Integration and Continuous Deployment (CI/CD) services.
2. Integration – This is a common environment where all developers commit code changes. The goal of this environment is to combine and validate the work of the entire project team, so work may be tested prior to promoting it to the Acceptance Environment.
3. Acceptance – This environment must be as identical to the production environment as possible. The purpose of the Acceptance environment is to simulate as much of the Production environment as possible. This environment is where User Acceptance type testing will be performed for each release. The Acceptance environment will also serve as a Demonstration/Training environment.
4. Production – This environment is where the APPLICATION software/capabilities are put into operation for end users.

System Architecture
The APPLICATION comprise a three-tier architecture

1) Client Tier
    a) Visualizations
2) Logic Tier:
    a) Model API
    b) Model Queue
3) Data Tier:
    a) Data

1.2 PURPOSE
For this solicitation, NRMC's purpose is to procure technical services to provide Operations and Maintenance for the APPLICATION.

1.3 SCOPE
The contractor shall provide comprehensive geospatial enterprise technical expertise and support services to include program and project management; systems engineering and lifecycle support; information management support; enterprise and technical architecture; data management; and operations and maintenance. This includes potential work surges to support changing priorities due to new and updated information technology and information sharing initiatives that support the evolving DHS mission.

1.4 OBJECTIVE
The objective of this contract is to provide technical service though the APPLICATION's lifecycle. The contractor will ensure the APPLICATION is compliant with all Federal/DHS/CISA requirements and criteria in accordance with all applicable Federal/DHS/CISA laws, executive orders policies, regulations, standards, and guidelines. The contractor shall also be responsible for operating and maintaining the APPLICATION and required documentation - as well as supporting the MCTE Program.

1.5 APPLICABLE DOCUMENTS

1.5.1 Compliance Documents
The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this contract:

1. Federal Information Security Management Act of 2014
   https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf 3.pdf
2. Section 508 of the Rehabilitation Act of 1973 (amended)
   https://www.gpo.gov/fdsys/pkg/USCODE-2011-title29/html/USCODE-2011-title29- chap16-subchapV-sec794d.htm
3. Federal Travel Regulations, General Services Administration
   https://www.gsa.gov/policy- regulations/regulations/federal-travel-regulation-ftr?asset=105444
4. Government Performance Results Act of 1993
   https://www.gpo.gov/fdsys/pkg/STATUTE- 107/pdf/STATUTE-107-Pg285.pdf
5. FIPS-140-2 Security Requirements for Cryptographic Modules.
6. FIPS-199 Standards for Security Categorization of Federal Information and Information systems.

7. NIST SP800-53 rev 4 Security and Privacy Controls for Federal Information Systems and Organizations.
8. DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified Information
9. DHS Management Directive 4300A Sensitive Systems Policy
10. DHS Management Directive 142-02-001 Information Technology Integration & Management
11. DHS Instructions 102-01-103 System Engineering Life Cycle (SELC)
12. DHS Management Directive 140-01 Information Technology Security Program Revision 2
13. DHS Management Directive 034-01 Geospatial Management
14. DHS Section 508 Compliance Test Process for Applications https://www.dhs.gov/publication/dhs-section-508-compliance-test-processes
15. DHS Instructions 102-01-001, Rev 01 Acquisition Management Instruction
16. DHS Management Directive 11056.1, Sensitive Security Information (SSI)
17. DHS Directive Number 121-01-001, Organization of the Office of the Chief Security Officer, DHS Instruction 121-01-011 DHS Administrative Security Program
18. DHS Instruction 121-01-007-01 Department of Homeland Security Personnel Security, Suitability and Fitness Program
19. DHS Privacy Incident Handling Guidance
20. DHS Instruction Manual 047-01-007, Rev # 03 Handbook for Safeguarding Sensitive Personally Identifiable Information; Handbook for Safeguarding Sensitive Personally Identifiable Information March 2012
21. DHS Instruction 047-01-001 Privacy Policy and Compliance
22. Directive Memorandum 140-09 DHS Privacy Impact Assessment Guidance
23. DHS Privacy Policy Guidance Memorandum 2011-02 Roles and Responsibilities for Shared IT Services
24. DHS System of Records Notices Official Guidance, April 2008
25. DHS 4300a ver.11-4.8.3.b Non-government furnished equipment restriction
26. DHS 4300A DHS Sensitive Systems Policy Directive, Version 13.1
27. DHS Instruction Number 264-01-002, Rev 01, DHS Counterintelligence Program
28. DHS Policy Directive 121-08 Requirements for Security Review of Foreign National Assignments and Overseas Employment
29. DHS Instructions Guide 026-06-001 Test and Evaluation Master Plan (TEMP)
30. DHS Policy Directive 121-04 Security Clearance Reciprocity
31. DHS Procedures for Operational Test and Evaluation of Cybersecurity
32. DHS Department of Homeland Security, National Protection and Programs Directorate, Office of Compliance and Security, Security Programs Division, Security Programs SOP, October 2017 http://dhsconnect.dhs.gov/org/comp/nppd/ocs/Pages/spd.aspx
33. MCTE security Plan and Procedure Policy

1.5.2 Reference Documents

The following documents may be helpful to the contractor in performing the work described in this BPA:

1. Public Law 107-296, “The Homeland Security Act of 2002” http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf
2. Public law 108-458, “The Intelligence Reform and Terrorism Prevention Act of 2004, Section 8201” https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW- 108publ458.pdf

3. Public Law 109-295, “Post-Katrina Emergency Management Reform Act of 2006’, Section 515. http://www.gpo.gov/fdsys/pkg/PLAW-109publ295/pdf/PLAW-109publ295.pdf
4. Public Law 107-347, “E-Government Act of 2002” http://www.gpo.gov/fdsys/pkg/PLAW- 107publ347/pdf/PLAW-107publ347.pdf
5. Public Law 104-106, Divisions D and E (as amended), “Clinger-Cohen Act of 1996” http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf
6. OMB Circular A-130, Management of Federal Information Resources: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a1 30revised.pdf
7. OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities: https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf
8. Federal Information Security Act and NIST: http://csrc.nist.gov/groups/SMA/fisma/index.html
9. Geospatial Line Of Business (GLoB): https://www.fgdc.gov/initiatives/geospatial-lob
10. Federal Enterprise Architecture Reference Models: https://obamawhitehouse.archives.gov/omb/e-gov/FEA
11. National Information Exchange Model (NIEM): http://www.niem.gov/
12. OMB Circular No. A-16, “Coordination of Geographic Information and Related Spatial Data Activities” https://obamawhitehouse.archives.gov/omb/circulars_a016_rev/
13. DHS Geospatial Data Model version 2.7: https://www.fgdc.gov/organization/working- groups-subcommittees/hswg/dhs-gdm/version-2-7
14. Federal Geospatial Platform: http://www.geoplatform.gov/
15. DHS Geospatial Concept of Operations: https://cms.geoplatform.gov/geoconops/geoconops-home
16. Computer Security Act of 1987: http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt
17. National Response Framework (3rd Edition)
18. National Infrastructure Protection Plan https://www.dhs.gov/national-infrastructure- protection-plan
19. National Protection Framework
20. National Disaster Recovery Framework
21. DHS Data Framework
22. U.S. Department of Homeland Security Continuity Plan, May 2017
23. National Cyber Incident Response Plan
24. Office of Infrastructure Protection Incident Management Plan

2.0 PROGRAM MANAGEMENT

2.1 TASK ONE – CLIN 0001. Program / Project Management Support

The contractor shall provide the program/project management support services necessary to maintain the technical direction and control of the service support effort required to accomplish the objectives of this SOW. Within 15 days of contract award, the contractor shall assume APPLICATION program management responsibilities to ensure the APPLICATION is compliant with all Federal/DHS/CISA requirements and criteria in accordance with all applicable Federal/DHS/CISA laws, executive orders policies, regulations, standards, and guidelines. . The contractor shall:

1. Plan, track, and manage program/project activities and maintain project documentation.
2. Draft correspondence, reports, and management plans for government review, acceptance and/or approval to include:
    a. Email or broadcast messaging and/or memoranda announcing new features, workshops, or initiatives for the APPLICATION.
    b. Reports on utilization and adoption of technology and data, the impact of programs, initiatives, or capabilities, or the potential for shared resources or reuse of existing DHS or inter-agency geospatial, analytical and data capabilities.
    c. Management plans including but not limited to roles and responsibilities, schedules, risk identification and mitigation for monitoring progress, achieving program objectives, and completing deliverables.
3. Support the coordination of schedules and/or facilitation of meetings, briefings, presentations, and technical demonstrations.
4. Provide graphic design and publishing expertise to enhance existing and/or draft new final reports, graphics, presentations, and web-enabled documents.
5. Develop and maintain training materials and user guides; execute DHS component/program office communication strategies and plans; assist with mission outreach; develop and assist with facilitating virtual webinars and ad-hoc training tutorials related to technology, tools, and capabilities supporting the APPLICATION.
6. Perform stakeholder and end user interviews and work sessions for the purposes of:
    a. Performing requirements gathering processes that include requirements definitions that translate user requirements into candidate capabilities for implementation into the APPLICATION. This process shall provide traceability from beginning to end.
    b. Documenting and assessing business objectives; conducting gap analysis of existing versus needed capability and identifying business requirements.
    c. Identifying and documenting points-of-collaboration, best practices, key resources and authoritative data sources.
7. Support the implementation of program/project methodologies (i.e., waterfall, iterative, Agile) and management of cost, schedule, and program/project performance.
8. Develop prescribed program/project and systems documentation as required by DHS Components' IT System Governance/Program Management directives.
9. Support DHS Governance of the APPLICATION to facilitate reviews, milestones, processes, decision-making and documentation for Acquisition Review Board (ARB); Enterprise Architecture (EA), Systems Engineering Life Cycle (SELC); Capital Planning and Investment Control (CPIC); and Planning, Programming, Budget and Execution (PPBE).
10. Support the knowledge transfer from outgoing contractors and undertake support of prior and ongoing tasks. The contractor shall make staff available for hands on facilitation so that the Government may receive continuous services.

3.0 TECHNICAL REQUIRMENTS/TASKS

3.1 TASK TWO – CLIN0002. System Engineering and Lifecycle Support

The contractor shall provide systems engineering and lifecycle APPLICATION support services. The contractor shall:

1. Perform system design, from development through decommissioning, to meet NRMC mission goals, objectives and evolving analytical requirements. Within 15 days of contract award, the contractor shall be capable of:
    a. Implementing enhancements of the APPLICATION.
    b. Updating system design based on evolving NRMC requirements and capacity increase.
2. Perform test and evaluation tasks to verify attainment of technical performance and validate required operational effectiveness and suitability of the APPLICATION during all lifecycle phases including:
    a. Develop testing criteria based on Operational Requirements and Key Performance Parameters.
    b. Develop test plans and test scripts to ensure that the integrity and security of the system(s) are adequately protected, and user requirements are met In Accordance With (IAW) DHS Procedures for Operational Test and Evaluation of Cybersecurity.
    c. Conduct Developmental and Operational Testing (DT & OT) as required by DHS Instruction Guide 026-06-001-01 Test and Evaluation Master Plan for government acceptance.
    d. Conduct modeling and simulations.
    e. Report testing conclusions and recommendations to support test results.
3. Provide solutions engineering, applications development and support services for the APPLICATION.

3.2 TASK THREE – CLIN 0003. Information Management and Support

The contractor shall provide information requirements analysis, collection, processing, production, acquisition, and analytic support services to meet a wide range of NRMC operational, functional, and business requirements. The contractor shall provide APPLICATION operational, functional, and technical support to include:

1. Analyze information requirements, processes, and existing available content catalogs.
2. Provide recommendations for collection or acquisition of information.
3. Acquire and/or collect information needed to satisfy NRMC operational, functional, business, and security handling requirements of acquired data.
4. Define geo-processing tasks (e.g. modeling and simulations), develop required content (e.g. web-based maps).
5. Provide analytic capabilities needed to satisfy NRMC specific mission support requirements.
6. Compile and maintain metadata on datasets, content, and products, ensuring data, content, and products are understandable and available in shareable formats.
7. Securely manage/classify all APPLICATION data IAW all applicable Federal/DHS/CISA guidelines.
8. Provide business process engineering and automated workflow development support.

3.3 TASK FOUR – CLIN 0004. Enterprise and Technical Architecture

The contractor shall provide APPLICATION enterprise technical architecture services. The contractor shall:

1. Provide architectural assessments while developing architectural products for the APPLCATION and NRMC operational business lines related to the APPLICATION.
2. Assess NRMC business objectives, conduct gap analysis of existing versus needed capability, and identify business requirements. Evaluate technical trends and provide recommendations for technology and architecture to meet business requirements and support analysis of alternatives for best fit.
3. Advise on network processing, data structures, data storage, data access, systems integration, IT security, and application interfaces and solutions for network problems.
4. Use architectural expertise to perform research on emerging technologies to support proof-of-concept (POC) capabilities and identify future solutions for NRMC operational business lines.
5. Develop, maintain, update and enhance APPLICATION standard operating procedures and concepts of operations in support of NRMC mission and goals.
6. Work with system engineers and solution architects to develop architecture plans that ensure the APPLICATION and solutions are optimized, resilient, scalable, interoperable, compliant with all DHS security requirements, documented, and based on open standards.
7. Ensure that all APPLICATION software is approved for use thought the DHS TRM process.

3.4 TASK FIVE – CLIN 0005. Data Management

The contractor shall provide technical data processing and maintenance, data management, data services and related strategies for data acquisition, archival and recovery, and implementation of various data repositories (graph, geodatabases. SQL, etc.) The contractor shall:

1. Perform data processing activities that support creation; curation; dissemination/information sharing; standardization; and decommissioning of various forms of data (e.g. GIS, graph, etc.).
2. Support government data information interoperability and archiving efforts to include (but not limited to): storage of information; querying of archived data; maintenance of data in open, accessible, available, and secure standards.
3. Design, implement and maintain a geo and non-geo database(s), which includes (but not limited to) design; architecture; metadata design, governance, system interconnects, creation, and maintenance; and repository creation.
4. Capture NRMC data management business needs and develop recommendations; implement; and operate and maintain long-term architecture solutions.
5. Perform work activities that support NRMC quality control and quality assurance to ensure the accuracy of contractor developed or modified geodatabases.
6. Evaluate reusability of current and operational data for additional analyses and processing.

7. Support CISA and NRMC program data management staff in understanding APPLICATION data architecture and information sharing and exchange such as:
    a. Reviews of DHS/CISA data methodologies and standards
    b. Assistance with development of SELC artifacts including data management plans, data models, requirements traceability, data quality, and data security documentation
    c. Participation at internal data and information exchange related meetings and working group sessions
    d. Feedback on data management or information sharing and exchange strategies

3.5 TASK SIX – CLIN 0006. Operations and Maintenance

The contractor shall provide operations and maintenance support for the APPLICATION. Support services include but are not limited to the following. The contractor shall:

1. Provide perfective, corrective and preventive maintenance on APPLICATION.
2. Implement and execute change and patch management, emergency fixes, security updates and vulnerability remediation.
3. Monitor the APPLICATION and related services.
4. Provide security support with Authority to Operate (ATO) artifacts and governance model activities such as monthly APPLICATION scans or associated reports.
5. Ensure that all CRITICAL/HIGH vulnerabilities are remediated in a timely manner according to DHS security guidance and policy.
6. Manage APPLICATION POA&M documentation and remediation processes as identified in DHS Security Authorization Terms and Conditions.
7. Provide development and deployment support for all APPLICATION modifications including upgrades or enhancements.
8. Provide infrastructure and network services support to be performed in coordination with DHS IT Services Offices, OnetNet, DHS Data Centers, government and/or commercial cloud providers, and other emerging government
9. Provide programmatic and/or engineering support renewal of data software, data, hardware, and services licensing, information sharing and/or interconnectivity agreements
10. Ensure that all software configurations are documented and compliant with all Federal/DHS standards and baselines.
11. Ensure that the standard baseline and configuration of software are documented and updated.
12. Ensure that all software for the APPLICATION is approved through the DHS TRM process.
13. Provide help desk support services including tracking and measuring performance of this service.
14. Provide report related to utilization of system components, web services, data feeds, other statistics such as unique visitors, length-of-visit, number of transactions, most frequently used, and so forth.
15. Perform quality assurance for the APPLICATION, solutions, applications and related services including configuration management processes that provides for

configuration identification, change control so that only approved and validated changes are incorporated into project documents and related system/software

3.6 TASK SEVEN – CLIN0007 (Optional). Transition to Classified Cloud Environment

If required to be executed the contractor shall provide support services to prepare for creating a classified version of the APPLICATION in an approved classified cloud environment. The contractor shall:

1. Support the implementation of classified version of APPLICATION leveraging various methodologies (e.g., waterfall, iterative, Agile).
2. Manage cost, schedule, and program/project performance.
3. Develop prescribed program/project and systems documentation as required by DHS Components' IT System Governance/Program Management directives.
4. Support DHS Governance of the APPLICATION to facilitate reviews, milestones, processes, decision-making and documentation for Acquisition Review Board (ARB); Enterprise Architecture (EA), Systems Engineering Life Cycle (SELC); Capital Planning and Investment Control (CPIC); and Planning, Programming, Budget and Execution (PPBE).
5. Provide architectural expertise in assessing and developing architectural design for classified APPLICATION
6. Assess NRMC business objectives, conduct gap analysis of existing versus needed capability, and identify business requirements related to classified APPLICATION

4.0 CONTRACTOR PERSONNEL

4.1 Qualified Personnel

The Contractor shall provide Labor Categories from the BPA to perform all requirements specified in this SOW to ensure the APPLICATION is compliant with all Federal/DHS/CISA requirements and criteria in accordance with all applicable Federal/DHS/CISA laws, executive orders policies, regulations, standards, and guidelines. .

4.2 Key Personnel

Certain experienced, professional and/or technical personnel are essential for successful accomplishment of the work to be performed under this SOW. These personnel are defined as "Key Personnel" and are those persons whose resumes are submitted for evaluation of the quotation. Personnel with contingency offers will not be accepted. The following Contractor personnel positions are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as Key at the time of award.

4.2.1 Project Manager Sr

The Contractor shall provide a Project Manager Sr. who shall be responsible for all Contractor work performed under this SOW. The Project Manager Sr. shall be the main point of contact for the Contracting Officer and the COR. It is anticipated that the Project Manager Sr. shall be one of the senior level employees provided by the Contractor for this work effort.

The Program Manager Sr. shall have experience with the execution and management of information technology programs. This includes direct experience in leading and executing IT solutions in DHS.

Experience Required

1. Shall have fifteen years of experience in managing IT projects with five of those managing DHS IT projects
2. Shall have experience managing cloud-based IT solutions
3. Shall have experience with DHS MD-102 Directives including Gate reviews
4. Shall have experience with DHS/CISA Security Authorization process
5. Shall have experience with DHS/CISA data standards
6. Shall have experience with DHS/CISA EA standards

Clearance/Suitability

Shall have active TS Clearance
DHS Suitability is required.

4.2.2 Project Manager Jr

The Contractor shall provide a Project Manager Jr. responsible for assisting the Project Manager Sr. in work performed under this SOW. The Project Manager Jr. shall be a secondary point of contact for the Contracting Officer and the COR.

The Program Manager Jr. shall have experience in executing information technology programs. This includes direct experience in executing IT solutions in DHS.

Experience Required

1. Shall have four years of experience working with IT projects - with two of those years managing DHS IT projects
2. Shall have experience managing cloud-based IT solutions
3. Shall have experience with Agile/Scrum for IT deployments
4. Shall have experience with Atlassian JIRA and Confluence

Clearance/Suitability

Shall have active TS Clearance
DHS Suitability is required.

4.2.3 GIS Visualization Developer

The Contractor shall provide a GIS Visualization Developer responsible for overseeing the APPLICATION's GIS visualization capabilities.

The GIS Visualization Developer shall have experience in GIS and related development.

Experience Required

1. Shall have ten years of experience in working with IT GIS projects
2. Shall have experience in Python, JavaScript and other modern technologies
3. Shall have experience in PostgreSQL
4. Shall have experience in managing GIS teams

Clearance/Suitability

4.3 Key Personnel Replacement

If replacement of key personnel is necessary, the contractor will provide prompt written notice of the proposed change to the COR and CO. If the change is a result of a non-emergency, the contractor shall provide the COR and CO two-week written notice. For changes that result from an emergency, the contractor shall provide prompt written notice to the COR and CO. The COR and CO have the right to accept or reject all personnel. The contractor and contractor's personnel must comply with all security requirements of this SOW including timely notification of changes in employment status for each staff member

4.4 Employee Identification

4.4.1 Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

4.4.2 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

4.5 Employee Conduct

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

4.6 Removing Employees for Misconduct or Security Reasons

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

provide the Contractor with a written explanation to support any request to remove an employee.

5.0 OTHER APPLICABLE CONDITIONS

5.1 Security

Some contractor personnel will be required to access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities under this SOW; therefore, some contractor employees will require DHS Fitness Determination to perform work. Other contractor personnel will not require access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities; therefore, those contractor employees will not require DHS Fitness Determination to perform work.

Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes one of the following categories of information:

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

B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or

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

Contractor access to classified information is not currently required under this SOW. However, the Government determines it needs to execute the optional Task Seven all applicable Contractor personnel will be required to have Top Secret clearances. Accordingly, all applicable Contractor employees provided for this requirement must be eligible for a Top Secret Clearance. The details will be provided in a Department of Defense (DD) Form 254 if necessary.

Post-Award Instructions Regarding Security Requirements For Contracts/Orders
The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

- Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.

- Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigation s will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement , addition, subcontractor employee, or vendor:
    a. Standard Form 85P, "Questionnaire for Public Trust Positions"
    b. FD Form 258, "Fingerprint Card" (2 copies)
    c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information
    Non-Disclosure Agreement"
    d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Rep01is Pursuant to the Fair Credit Reporting Act"

- Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.
- DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office.
- Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.
- The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.
- When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall

provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- The POC at the Security Office is:
    - DHS Office of Security
    - Personnel Security Staff
    - Attn: Ronnie Mitchell
    - Washington DC 20528
    - Telephone: (202) 447-5372

5.2 Period of Performance

The period of performance for this contract is a one-year base period with three one-year option periods as follows:

5.3 Place of Performance

The primary place of performance will be the Contractor's facilities or normal workplace with frequent visits to the Department of Homeland Security at 4200 Wilson Blvd., Arlington, VA 22203

5.4 Contractor Telecommuting – Remote Personal Residence Work Locations
Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission. With approval of the APPLICATION PM, telecommuting is permitted for onsite personnel under the task order in accordance with the requirements below.

The provision to permit contractor telecommuting may be revoked at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.

5.5 Hours Of Operation
Contractor employees shall generally perform all work between the hours of 0800 and 1600 EST, Monday through Friday (except Federal holidays). However, there may be

occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

5.6 Travel
See Section 7.7 of the RFQ.

5.7 Post Award Conference
The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 15 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at 4200 Wilson Blvd., Arlington, VA 22203 or via teleconference.

5.8 Project Plan
The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 30 business days after the Post Award Conference.

5.9 Business Continuity Plan
The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 60 business days after the date of award and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

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

5.9.1
The Contractor Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 2 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately make contact with the Contractor Project Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)

- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

5.9.2
The Government and Contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

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

5.11 Progress Meetings
The Project Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at 4200 Wilson Blvd., Arlington, VA 22203.

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

5.13 Protection of Information
The Government will provide all necessary information, data and documents to the Contractor for work required under this contract.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

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.

Contractor access to proprietary information 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.

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

Contractor access to Chemical Vulnerability Information (CVI) and Protected Critical Infrastructure Information (PCII) is required. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

CVI is the information protection designation authorized by Section 550 of Public Law 109-295, “Department of Homeland Security Appropriations Act of 2007,” to protect information from inappropriate public disclosure. This includes information that is developed and/or submitted to DHS pursuant to the Chemical Facility Anti-Terrorism Standards (CFATS) regulation which implements Section 550. Chemical facility managers expect that the information provided to DHS will be protected from public disclosure or misuse and that individuals in possession of CVI will safeguard the information in accordance with the following statutory requirements:

Defining CVI
The following information (whether written, verbal, electronic, digital, or otherwise) is CVI:
• Security Vulnerability Assessments (SVA);
• Chemical Site Security Plans (SSP);
• Documents relating to the Department's review and approval of Security Vulnerability Assessments and Site Security Plans, including:
    o Letters of Authorization;
    o Letters of Approval and responses thereto;
    o Written notices; and
    o Other documents developed pursuant to SVA and SSP.
• Alternative Security Programs;
• Documents relating to inspections or audits of chemical sites;
• Any records required to be created or retained by a covered facility;
• Sensitive portions of orders, notices or letters relating to SVA or SSP;
• Information developed pursuant to SVA and SSP (such as the Chemical Security Assessment Tool (CSAT) Top-Screen and the determination by the Assistant Secretary that a chemical facility presents a high level of security risk); and
• Other information developed for chemical facility security purposes that the Secretary, in his discretion, determines is similar to the information in SVA or SSP.

Handling CVI
CVI will be marked, stored, transmitted and destroyed in accordance with the procedures outlined in the Procedural Manual, “Safeguarding Information Designated as CVI.” CVI must be appropriately designated, withheld from public disclosure and

physically controlled and protected. Copies of CVI or derivative products are subject to the same protections as original CVI. NPPD Personnel should direct questions and requests for the manual to the Chemical Facility Anti-Terrorism Standards (CFATS) Helpdesk (CFATS@hq.dhs.gov).

Defining PCII

PCII is a subset of Critical Infrastructure Information (CII) that is voluntarily shared by critical infrastructure owners and operators within the government to analyze data, security critical infrastructure, identify vulnerabilities, develop risk assessments and enhance recovery preparedness measures. CII is defined in 6 U.S.C., Section 131(3) (Section 212(3) of the Homeland Security Act) as information not customarily in the public domain that is related to the security of critical infrastructure or protected systems. PCII is protected from disclosure through the Freedom of Information Act (FOIA); similar state and local disclosure laws; use in regulatory actions; and use in civil litigation.

PCII must be validated by a PCII Officer, Deputy Officer or Designee and must indicate the following:

• Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

• The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; and

• Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Handling PCII

PCII will be marked, stored, transmitted and destroyed in accordance with the procedures outlined in the Procedural Manual, “Protected Critical Infrastructure Information Program Procedures Manual” (PCII-Assist@hq.dhs.gov). PCII must be appropriately designated, withheld from public disclosure and physically controlled and protected. NPPD Personnel should direct questions and requests for the manual to the PCII Helpdesk (PCII-Assist@hq.dhs.gov).

5.14 Section 508 Compliance

(a) 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.

(b) 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.

(c) When providing and managing hosting services for ICT, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance before providing the hosting service.

(d) When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

(e) When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat

(f) When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

(g) When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/508-testing. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/trusted-tester.

(h) When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/508-testing.

(i) When developing or modifying software that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the contractor shall ensure software can be used to create electronic content that conforms to the Section 508 standards.

(j) Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

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

5.14.1 Instructions to Offerors

(a) For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The

Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

(b) The offeror shall describe plans for features that do not fully conform to the Section 508 Standards.

5.14.2 Acceptance Criteria

(a) Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:

- Accessibility test results based on the required test methods.
- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation on how to configure and install the ICT Item to support accessibility.
- Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

(b) Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

5.15 DHS Geospatial Information System Terms and Conditions

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

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

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

6.0 GOVERNMENT TERMS & DEFINITIONS

- A-LAN – DHS unclassified network
- C-LAN – DHS classified network
- CI – Critical Infrastructure
- CONUS – Continental United States
- COP – Common Operating Picture
- COR – Contracting Officer's Representative
- DHS – Department of Homeland Security
- EA – Enterprise Architecture
- EOD – Entry on Duty

- FEMA – Federal Emergency Management Agency
- GA – Geospatial Analyst
- GEOINT- Geospatial Intelligence
- GSA - General Services Administration
- GIS – Geographic Information System
- HILFD – Homeland Infrastructure Foundation-Level Database
- HSDN – DHS secret network
- IAC – Integrated Analysis Cell
- I&A – Intelligence and Analysis
- IICD – Infrastructure Information Collection Division
- iRAC- Incident Risk Analysis Cell
- NAC – Nebraska Avenue Complex
- NCR – National Capital Region
- NGA – National Geospatial – Intelligence Agency
- NIPP- National Infrastructure Protection Plan
- NRMC – National Risk Management Center
- OPM – Office of Personnel Management
- PCII – Protected Critical Infrastructure Information
- PM – Project Manager
- PMO – Project Management Office
- POC – Proof-of-Concept
- PSA – Protective Security Advisor
- SOW – Statement of Work
- QC – Quality Control
- RA – Regional Analyst
- RFI – Request for Information
- RRAP – Regional Resiliency Assessment Program
- RD – Regional Directors
- SEAR – Special Event Assessment Rating
- SOP – Standard Operation Procedure

7.0 **GOVERNMENT FURNISHED RESOURCES**

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

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

7.1 Property Inventory

Contractor must establish and maintain an accurate master inventory of all property purchase for CISA under this Contract.

7.2 Monthly Asset Management Report

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

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

8.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 7.0.

8.1 Property Inventory

The Contractor will ensure personnel apply a DHS-supplied barcode to all property purchased for CISA. Contractor/Servicing Agency must establish and maintain an accurate master inventory of all property purchase for CISA under this Contract.

8.2 Notification of Property Receipt

Contractor will confirm receipt of CISA property purchased under this SOW with the assigned CISA Accountable Property Officer (APO) and COR within 5 business days of receipt.

APO Name & Contact Information

8.3 Monthly Asset Management Report

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

- DHS Barcode
- Acquisition Date
- Acquisition Status
- Asset Condition
- Manufacturer Name
- Manufacturer Model
- Asset Description
- Serial Number
- Asset Cost
- Locationb

8.4 Invoice/Receipts

Contractor will ensure copies of all invoices/packing slips/receipts for property purchased for CISA accompanies the Monthly Asset Management Report.

9.0 GOVERNMENT ACCEPTANCE PERIOD

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

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

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

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

10.0 DELIVERABLES

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

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.6	**Post Award Conference**	15 Business Days After Contract Award	N/A
2	4.6, 4.7	***Draft Contractor Project Plan***	30 Business Days After Contract Award	COR, Contracting Officer
3	4.7	**Final Contractor Project Plan**	45 Business Days After Contract Award	COR, Contracting Officer
4	4.8	**Original Business Continuity Plan**	60 Business Days After Contract Award	COR, Contracting Officer
5	4.8	**Updated Business Continuity Plan**	75 Business Days After Contract Award	COR, Contracting Officer

Attachment 1

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
6	4.9	**Progress Reports**	Monthly	COR, Contracting Officer
7	6.1, 7.1	**Master Inventory Report**	Monthly	COR, APO
8	7.2	**Receipts for Purchased CISA Property**	Within 5 Business days of purchase	COR, APO
9	6.2, 7.3	**Monthly Asset Management Report**	Monthly	COR, APO
10	7.4	**Invoices/packing slips/receipts for property purchased for CISA**	Monthly with the Asset Management Report	COR, APO
11	2.1	**Sprint Planning Meeting Report**	Monthly	Program Manager
12	2.1	**Sprint Meeting Results**	Monthly	Program Manager