DEPARTMENT OF HOMELAND SECURITY (DHS)

CYBERSECURITY AND INFRASTRUCTURE SECURITY (CISA)

Statement of Work (SOW)
for
Digital Transformation Support Services (DTSS)

May 9, 2023

1.0 GENERAL

1.1 BACKGROUND

CISA's mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA includes the CISA Mission Enabling Offices (MEOs) and six Divisions: the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Integrated Operations Division (IOD), Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered within the National Capital Region (NCR).

1.2 BLANKET PURCHASE AGREEMENT (BPA) STRUCTURE

This BPA will be fulfilled through orders for support services across the various task area requirements within the Statement of Work (SOW). The following sections describe the high-level scope of the overarching BPA and task areas. Any combination and volume of functional area services may be acquired for a given order according to the government's instructions and scope of work. Individual orders may include one or more task areas and may include either firm fixed price (FFP), time and materials (T&M), or labor hour (LH) orders, depending on the scope and timelines of the products[1] and services required. Given the importance of long-term success for this effort, the term of the BPA will be a 12-month base period, with four 12-month option periods.

The requirements specified in this BPA provide a broad overview of tasks forthcoming on Orders. Detailed specifications on standards, agile methodology types, and products leveraged or requiring purchase will be detailed in Orders. Examples of some products and specifications that may be leveraged can be found in the individual Task Areas

1.3 SCOPE

Given the dynamic nature of the CISA mission and significant increase in both authorities and funding, the scope is intended to be both broad and flexible in accommodating unforeseen change across CISA to include CISA OCIO, MEOs and Divisions. CISA requires digital transformation support services, which include the following:

- Providing support for organizational governance and delivery of core enterprise capabilities. Being able to have a consistent baseline of service excellence measured by impact to productivity and responsiveness of CISA headquarters teams and CISA mission Divisions to cybersecurity and infrastructure preparedness initiatives.
- Establishing OCIO as a source for cross-agency coordination and collaboration on established and emerging technology needs that impact CISA's mission demands.
- Having the capability for mission focused, data driven innovation, including methods for rapid evaluations, testing and adoption of new technologies.

[1] The product is not a commodity like a printer; rather, this requirement concerns digital services, and products would be a digital application or a digital Minimum Viable Product (MVP).

- Having the ability to establish transparency and accountability in the planning, delivery, and completion of large-scale enterprise-wide IT initiatives.
- Giving CISA the capability for enterprise IT management practices and capabilities to reflect current trends in project management, infrastructure cybersecurity, service delivery, and cloud adoption.
- Being capable to innovate and rapidly execute as a unified agency across mission divisions.
- Being able to structure, control the process, and manage the overall capability for IT infrastructure for rapid responsiveness to emerging threats and technology capabilities.

The SOW consists of five (5) Task Areas:

- Task Area 1: Program Management
- Task Area 2: Transformation Strategy, Enablement, and Service Experience Support
- Task Area 3: Digital Solution Development, Automation, and Infrastructure Support
- Task Area 4: Enterprise Data Management and Analytics Support
- Task Area 5: Operations and Sustainment

1.4 OBJECTIVE

CISA is seeking to implement innovative transformation technologies and support services to establish and acquire CISA Digital Transformation Support Services with individual orders to address several current and anticipated challenges across the agency such as the following:

- **Lack of CISA centrally developed and deployed digital services-** As the mission and requirements of the agency continue to evolve, CISA must have the flexibility and agility to centrally innovate and deploy digital services at speed.
- **Disparate business and mission systems-** Core business systems vary widely across the agency which leads to incapability and inconsistency of systems. This impacts CISA's ability to integrate the organization, streamline business operations, and maintain visibility into the status of basic business operations.
- **Disparate data management, analytics, and collaboration environments-** CISA data assets are spread across and outside the agency. CISA collaboration environments vary across the agency and, in most cases are inoperable and not consistent. This impacts CISA's ability to achieve its full mission through an operating model that enables an agency-wide approach to operational issues.
- **Insufficient mechanisms to move quickly-** CISA has access to commodity-type IT services but lacks a CISA owned contract vehicle with the mechanism to quickly add technical SMEs and standup digital services required to test, prototype, and transform the agency's IT capabilities rapidly.
- **Enterprise IT governance and stakeholder engagement-** CISA requires the ability to engage internal agency stakeholders, identify common needs, and plan and implement enterprise-wide solutions in a coordinated manner.

1.5 PERIOD OF PERFORMANCE

Base Period	July 17, 2023, through July 16, 2024
Option Period One	July 17, 2024, through July 16, 2025
Option Period Two	July 17, 2025, through July 16, 2026
Option Period Three	July 17, 2026, through July 16, 2027
Option Period Four	July 17, 2027, through July 16, 2028

1.6 PLACE OF PERFORMANCE

The primary place of performance will be a combination of CISA OCIO 4601 N. Fairfax Ave, Arlington, VA 22203, the Contractor's facilities, and other CISA facilities in the Washington, DC Metro Area. The specific location will be indicated in each individual order.

All classified work will be performed at the Government facilities and/or Government SCIF.

1.7 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 0800 and 1600 ET, 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.

The Contractor shall typically work eight hours a day, 5 days a week, but may be required to work beyond this typical schedule. Any alterations to the work schedule shall be negotiated with the COR. Contractor personnel shall be available for weekend and after-hours work as directed by the COR and may be called upon for after-hours emergencies.

1.8 HOLIDAYS AND ADMINISTRATIVE LEAVE

CISA personnel observe the following days as holidays (non- business):

- New Year's Day
- Martin Luther King Jr.'s Birthday
- Presidents' Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veterans Day
- Thanksgiving Day
- Christmas Day

CISA personnel also observe any other day designated by Federal statute, Executive Order, or the President's proclamation. When any observed holiday falls on a Saturday, the preceding Friday is observed. When any such day falls on a Sunday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule, period of performance, or adjustment to the price, except as set forth in the order. Except for designated around-the-clock or emergency operations, Contractor personnel

will not, without written consent from the COR, be able to perform work on-site under the order with CISA on the holidays set forth above. The Contractor will not charge any holiday as a direct charge to the order. In the event that Contractor personnel work during a holiday other than those listed above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost.

In the event CISA grants administrative leave to its Government employees at the site, on-site Contractor personnel shall also be dismissed if the site is being closed. However, the Contractor shall continue to provide sufficient personnel to perform critical efforts already in progress or scheduled and shall be guided by the instructions issued by the order or her/his duly appointed representative. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances, the Contractor shall direct its staff as necessary to take actions such as reporting to its own site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Contractor for the period of any such site closure are a reimbursable item of direct cost under the contract order for employees whose regular time is normally a direct charge if they continue to perform contract work; otherwise, costs incurred because of site closure are reimbursable as indirect costs in accordance with the Contractor's established accounting policy.

Work may only be performed on a federal holiday and/or at the Contractor's site with prior written consent of the COR.

1.9 OVERTIME

This contract is subject to the Services Contract Act of 1965. Contractor personnel may not work more than forty (40) hours a week without prior written approval of the COR. Approved overtime hours shall be invoiced at the normal hourly rate for this effort.

1.10 TRAVEL

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

1.11 APPLICABLE DOCUMENTS

1.11.1 COMPLIANCE DOCUMENTS

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

- Federal Information Security Modernization Act of 2014 https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
- Section 508 of the Rehabilitation Act of 1973 (amended) https://www.govinfo.gov/content/pkg/USCODE-2011-title29/pdf/USCODE-2011-title29-chap16-subchapV-sec794.pdf
- Federal Travel Regulations, Code of Federal Regulations https://www.ecfr.gov/current/title-41/subtitle-F
- Government Performance Results Modernization Act of 1993 https://www.congress.gov/103/statute/STATUTE-107/STATUTE-107-Pg285.pdf
- FIPS-140-2 Security Requirements for Cryptographic Modules.
- FIPS-199 Standards for Security Categorization of Federal Information and Information systems.
- NIST SP800-53 rev 4 Security and Privacy Controls for Federal Information Systems and Organizations.
- DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified Information
- DHS Management Directive 4300A Policy Directive (Version 13.2, September 20, 2022)
- DHS Management Directive 142-02-001 Information Technology Integration & Management
- DHS Instructions 102-01-103 System Engineering Life Cycle (SELC)
- DHS Management Directive 140-01 Information Technology Security Program Revision 2
- DHS Management Directive 034-01 Geospatial Management
- DHS Section 508 Compliance Test Process for Applications https://www.dhs.gov/publication/dhs-section-508-compliance-test-processes
- DHS Management Directive 11056.1, Sensitive Security Information (SSI)
- DHS Directive Number 121-01-001, Organization of the Office of the Chief Security Officer, DHS Instruction 121-01-011 DHS Administrative Security Program
- DHS Instruction 121-01-007-01 Revision 01, Department of Homeland Security Personnel Security, Suitability and Fitness Program
- DHS Instruction Guide 047-01-008 Revision 00.1 Privacy Incident Handling Guidance
- DHS Instruction 047-01-001 Privacy Policy and Compliance
- DHS Privacy Policy Guidance Memorandum 2011-02 Roles and Responsibilities for Shared IT Services
- DHS Privacy Policy Guidance Memorandum 2008-02, DHS Policy Regarding Privacy Impact Assessments, December 30, 2008
- DHS Instruction Manual 047-01-007, Rev # 03 Handbook for Safeguarding Sensitive Personally Identifiable Information; Handbook for Safeguarding Sensitive Personally Identifiable Information December 4, 2017
- DHS Instruction 047-01-001 Privacy Policy and Compliance
- Directive Memorandum 140-09 DHS Privacy Impact Assessment Guidance
- DHS System of Records Notices Official Guidance, April 2008

- DHS 4300a ver. 13.2, September 20, 2022-4.8.3.b Non-government furnished equipment restriction
- DHS 4300A DHS Sensitive Systems Policy Directive, (Version 13.2, September 20, 2022)
- DHS Instruction Number 264-01-002, Rev 01, DHS Counterintelligence Program
- DHS Policy Directive 121-08 Requirements for Security Review of Foreign National Assignments and Overseas Employment
- DHS Instructions Guide 026-06-001 Test and Evaluation Master Plan (TEMP)
- DHS Procedures for Operational Test and Evaluation of Cybersecurity
- DHS Management Directive (MD) 4010.2: Section 508 Program Management Office Electronic and Information Technology Accessibility.
- Homeland Security Enterprise Architecture (HLS EA), current version.
- Office of Management and Budget M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007

1.11.2 REFERENCE DOCUMENTS

The following documents may be helpful to the Contractor in performing the work described in this document:

- Federal Information Technology Acquisition Reform Act (FITARA), 2015: [2]
  - Provides the statutory basis for Federal-wide IT reform
- Federal Information Technology Shared Services Strategy, May 2, 2012: [3]
  - Provides organizations in the Executive Branch of the United States Federal Government (Federal Agencies) with policy guidance on the full range and lifecycle of intra- and inter-agency IT shared services that enable mission, administrative, and infrastructure-related IT functions.
- Federal CIO 25 Point Implementation Plan to Reform Federal Information Technology Management, Dec 9, 2010: [4]
  - Specifies that "Agencies must focus on consolidating existing data centers, reducing the need for infrastructure growth by implementing a Cloud First policy for services, and increasing the use of available cloud and shared services".
- Federal Risk and Authorization Management Program (FedRAMP): [5]
  - Provides joint "provisional" authorizations and continuous security monitoring services applicable to "Executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies, including systems provided or managed by other departments or agencies, contractors, or other sources".

[2] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291.
[3] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf.
[4] https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf
[5] https://www.fedramp.gov/about-us/about/

- Federal Cloud Computing Strategy, Feb 8, 2011: [6]

1.11.3 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

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

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

1.11.4 GEOSPATIAL INFORMATION SYSTEM TERMS AND CONDITIONS

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

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

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

1.11.5 EPEAT AND ENERGY STAR LANGUAGE

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

[6] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

1.11.6 THE HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)

The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

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 Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card."

1.12 TRAINING

All contract personnel are required to complete the CISA mandatory training courses by the mandatory due date(s). The Contractor is responsible for maintaining records of contracting employees that have completed the mandatory training and provide semimonthly updates to the COR on the 1st and 15th day of each month or the next business day if the 1st or 15th is a Holiday or on the weekend. The Contractor is also responsible for providing copies of the training certificates to the COR when requested.

1.13 CLEARANCE PROCESS/CONTRACTOR SUITABILITY

The following information is provided to prospective offerors who have never worked with CISA before, or for those who do not have knowledge of the background investigation process. Information provided is based upon averages and is meant to provide a basis for estimating the time it may take to clear resources and begin work.

The background investigation (BI) process within the CISA begins when the contractor submits the Contract Employee Initial Background Investigation Form (Form 77), Background Investigations Requirements Determinations (BIRD) form, Fair Credit Reporting Act release form and the new contractor information sheet to the Government. The Government approved paperwork is then submitted to Internal Affairs (IA) for a determination regarding whether the applicant is eligible for 1) reciprocity, or 2) needs to be invited into e-QIP. CISA IA will review the BIRD request, along with attachments, to conduct the appropriate systems check to render the appropriate determination, i.e., initiation required, reciprocity eligible, reactive, reciprocity revoked. This determination process takes approximately 1 week.

- If candidate is eligible for reciprocity, the process to a full background investigation averages about 1 month.

- If the determination rendered was "Initiation Required" or "Reciprocity Revoked", the Government will be responsible for taking the appropriate action to allow the applicant access to e-QIP. The applicant will need to complete e-QIP, financial disclosure forms and fingerprint cards. This process takes approximately one week, however the applicant has up to 30 days. All forms are submitted to the Government for review. If all forms and e-QIP are completed, the BI package is submitted to IA. If not, e-QIP is rejected and must be corrected. After submitting the BI package to IA, the BI is conducted. An Interim BI is the next step in the process and averages approximately 30-45 days. A full BI averages approximately 60-90 days after the Interim BI is granted. Please note that this is the best-case scenario, applicants may drop into Delay, which means that more documentation is required for the BI to be completed. Delayed applicants can remain in delay for many months and may be found unsuitable and therefore unable to be hired onto the contract. From submission of documentation to a delay determination usually averages one to two months.

Overall, the average time to receive a Full BI, from submission of the required BI documents, is 104 days. This time estimate is furnished for the purposes of indicating the time required to obtain CISA BI cleared personnel. This is the Government's estimate and is not intended to be binding on either party or to be the only possible scenario.

2.0 SPECIFIC REQUIREMENTS/TASKS

Contractor will require access to classified information at the Top-Secret level under this SOW. The maximum level of classification is Top Secret/Sensitive Compartmented Information (TS/SCI). Access to classified information will be specified in a Department of Defense Contract Security Classification Specification (DD Form 254) issued with the resultant order (s), if applicable. FAR 52.204-2 Security Requirements is applicable to this BPA and resultant order(s).

Vendors must have a DCSA issued Top Secret facility clearance at quote submission and maintained through the life of the BPA.

At the time of BPA award the following personnel are required to possess a Top Secret (TS) Clearance: The BPA Program Manager and Project Managers for the orders. They must also be eligible to obtain and retain Sensitive Compartmented Information (SCI) access provided by DHS, throughout the BPA period of performance.

All other contractor personnel will require access to Unclassified FOUO information.

2.1 TASK AREA 1. Program Management

The Contractor shall provide services to continuously manage and track adequate levels of project management, technical resources, quality assurance, scheduling, cost, budget, and financial controls throughout the performance of this BPA. The Contractor shall plan, direct, control, measure, monitor, and report to the Government on all activities of the working requirements. The Contractor shall ensure that all personnel are provided the necessary program management tools, guidance, plans, processes, procedures, and resources that shall enable the Contractor to comprehensively manage the BPA and individual orders.

2.1.1 CONTRACTOR TRANSITION-IN

The Contractor transition-in period shall begin upon receipt and acceptance of the contractor's Transition Plan by the Contracting Officer (CO). The transition-in period shall cause no disruption in development and especially Operational & Maintenance (O&M) services of existing applications.

The approved transition-in plan and schedule (updated to reflect any agreements made at the Kickoff Meeting) shall be submitted to the CO/Contracting Officer's Representative (COR) within 10 days after Kick Off meeting unless otherwise directed by the CO. The Contractor shall account for 5 working days of Government review and approval of the transition backlogs prior to executing the transition.

The Transition Plan should include, at minimum:

- Contractor shall agree that all deliverables, products, licenses, designs, data, documentation, tests, user research notes, source code, configuration settings and files, and materials developed through this BPA will be the property of CISA
- Transition roadmap
- Identify transition risks and risk mitigation
- Define roles and responsibilities with an initial Staffing Plan
- Define a knowledge transfer approach
- Provide checklist of transition activities and milestones
- Schedule of events and timelines
- Communication Plan/Strategy
- Innovation and Research methodology/strategy
- On-Call / Production Support Strategy

The contractor transition-in progress shall be provided in the weekly status report and provide information on all requirements in the transition-in plan. The Government reserves the right to call meetings at any time during the transition-in period to review all transition requirements.

2.1.2 WEEKLY STATUS REPORTS

The Project Manager shall provide a Weekly Status report to the COR and all Technical Monitors (if assigned) via electronic mail on a weekly basis (Monday from the previous week). This report shall include a summary of all Contractor work performed, an assessment of technical progress, schedule status, meetings attended, and any Contractor concerns or recommendations for the previous period.

Weekly status reports shall reflect the status of each task, at a minimum:

a) Reporting period.
b) Progress/status.
c) Current week activities.
d) Risk and Mitigation Strategy; and,
e) Forecast of next week's activities to include any anticipated risks or problems, along with recommended mitigation strategies.

2.1.3 MONTHLY FINANCIAL REPORT:

The Program Manager shall submit a Monthly Financial Report by the 25th of the month to the COR via electronic mail at the time of Invoicing.

2.1.4 ORGANIZATIONAL CHARTS

The contractor shall provide and maintain an Organizational Chart monthly showing resource assignments and coverage for in-scope applications. As the priorities and requirements drive re-assignments, the Organizational Chart shall be updated and submitted to the COR by the 25th of the month.

2.1.5 CONTRACTOR TRANSITION-OUT

At the completion of performance of this BPA, the Contractor shall fully support the transition-out of the Contractor's work that is turned over to another entity, either Government or a successor offeror(s). The Contractor shall assist with transition planning and shall comply with transition milestones and schedule of events.

The Contractor shall be responsible for the implementation of the transition and application cut over activities.

The Contractor shall be responsible for the transition-out of all technical activities identified in this BPA. As part of the transition-out, the Contractor shall be responsible for:

- Inventory and orderly transfer of all Government Furnished Property (GFP), to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)

- Transfer of documentation currently in process
- Transfer of all software code in process
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to participate in transition management
- Identify transition risks and risk mitigation

The Contractor shall submit a Transition-Out Plan to the CO/COR, 120 days prior to the BPA or order expiration date. The Transition-Out Plan shall include support activities for all transition-out efforts for follow-on requirements to minimize disruption of services. The Transition-Out Plan shall:

- Identify equipment, hardware, software, documents, and other artifacts that are included in the transition
- Establish roadmap and backlogs
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide checklists
- Transition milestones and schedule of events

The Contractor shall account for a 10-business day Government review process prior to executing the transition. Upon award of a follow-on BPA or order, the incumbent Contractor will work with the new Contractor to provide knowledge transfer and transition support, as required by the COR and Program Manager and/or Project Manager.

2.1.6 BUSINESS CONTINUITY PLAN (BCP)

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the CO/COR. The BCP shall be due 15 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

Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 4 hours of activation or as directed by the Government, and shall be sustainable until the emergency is resolved and normal conditions are restored or the BPA is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately contact the Contractor Program Manager to ascertain the status of any Contractor personnel who were working in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Program Manager and the COR shall promptly open an effective means of communication and verify:

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

The Government and Contractor Program 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 BPA. Regardless of Call Order type, and of work location, Contractors performing work in support of authorized tasks within the scope of their BPA shall charge those hours accurately in accordance with the terms of this BPA.

2.1.7 PROGRESS REPORTS

The Program Manager shall provide consolidated monthly progress report(s) of awarded Order(s) to the COR via electronic mail by the 25th of the month. 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.

2.1.8 PROGRESS MEETINGS

The Program 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 the Government's facility or via teleconference.

2.1.9 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 (Microsoft Office Applications).

2.2 TASK AREA 2. TRANSFORMATION STRATEGY, ENABLEMENT, AND SERVICE EXPERIENCE SUPPORT

CISA is seeking to establish cross-program consistency, reuse, common architectures, security standards and other scalable practices for solutions that are used across the agency. To maximize the potential of current and planned IT capabilities, CISA requires transformation strategy and enablement, and service experience support services to centrally establish required standards and services and enable adoption across currently disconnected programs and mission groups. The contractor will augment an existing staff of both Government and other contractors and will facilitate as integrators working together cohesively across function and organizational boundaries. The contractor shall develop and implement a standardized framework for engaging CISA teams and stakeholders, CISA information system users, and mission stakeholders to identify priorities, improve service design effectiveness, and establish consistent end user experiences. The contractor shall provide design thinking and user experience strategy, consulting, design, and implementation support to CISA teams with a concentration on organizational effectiveness, accountability, and continuous improvement in service delivery.

Except as provided under 6 U.S.C. 396, no entity performing lead system integrator functions in the acquisition of a major system (See (HSAR) 48 CFR 3002.101) by DHS may have any direct financial interest in the development or construction of any individual system or element of any system of systems under the program in which the entity is performing lead system integrator functions.

2.3 TASK AREA 3. DIGITAL SOLUTION DEVELOPMENT, AUTOMATION, AND INFRASTRUCTURE SUPPORT

CISA requires flexibility and agility to innovate, deploy and evolve capabilities at speed as its mission and agency requirements continue to evolve in its execution of infrastructure and system architecture, design, implementation, integration, and maintenance. The Contractor shall support CISA with the adoption of new digital solutions to support achieving the economies of scale that support the business case for digital platforms and requires support to achieve CISA's goals. The contractor shall employ Development, Security, and Operations (DevSecOps) with the use of principles such as Infrastructure as Code (IAC) and Continuous Integration/Continuous Deployment (CI/CD) pipelines to make infrastructure environments available on demand with the necessary security accreditation built in to provide the delivery of mission and business value to end users with higher quality solutions and technical maturity. The Contractor's software development shall be delivered in an incremental, fast-paced style to reduce the risk of failure. The Contractor shall deliver working software into users' hands as early as possible to give the design and development team opportunities to adjust based on user feedback about the service. A critical capability is being able to automatically test and deploy the service so that new features can be added often and be put into production easily. Development practices shall employ practices such as design and code in sections, automated testing, verifying code against Common Weakness Enumeration (CWE), Common Vulnerabilities Exposures (CVE), Open Worldwide Application Security Project (OWASP) to identify and remedy code vulnerabilities, test automation, issue resolution, and prototyping.

2.4 TASK AREA 4. ENTERPRISE DATA MANAGEMENT AND ANALYTICS SUPPORT

CISA requires transparency into decision-making with data-driven technical and organizational approaches. The contractor shall support establishing and implementing a comprehensive CISA data architecture, the design and engineering of consolidated and consistent cross-agency data management solutions, development and deployment of data integration analytics solutions, and the design and development of end-user data visualization capabilities for CISA stakeholder organizations. The Contractor shall provide technology solutions which enable development teams to work efficiently and enable services to scale easily and cost-effectively. Recommendations for choices for hosting infrastructure, databases, software frameworks, programming languages and the rest of the technology stack shall seek to avoid vendor lock-in and match what successful modern consumer and enterprise software companies would choose today. In particular, the vendor shall consider using open source, cloud-based, and commodity solutions across the technology stack.

2.5 TASK AREA 5. OPERATIONS AND SUSTAINMENT

The Contractor shall perform ongoing operations and standardization of CISA Operations and Maintenance for cloud-based Software of a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) solutions, where required, to allow end-user insights and operational feedback to guide continuous improvement of the platform configurations and feature sets. Cloud-based solutions may include but is not limited to those utilizing Amazon Web Service (AWS), Microsoft Azure, Google Cloud Platform, ServiceNow, Atlassian, Appian, Apple AppStore, and Google Play Store. The Contractor shall deploy services on a flexible infrastructure, where resources can be provisioned in real-time to meet spikes traffic and user demand. The Contractor shall perform defect resolution and corrective maintenance categorized as break/fix. In instances where newly developed or enhanced applications interact with legacy systems, the Contractor is expected to collaborate with the legacy maintainer to troubleshoot issues and provide information to the Government. The Government and the Contractor shall collaborate and identify what corrective action is required.

2.6 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the CO and COR no later than 14 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the CO, is to discuss technical and contracting objectives of this BPA and review the Contractor's draft project plan. The Post Award Conference will be via teleconference.

2.7 PROJECT PLAN

Project Plans for each order may be required. The Contractor shall provide a draft Project Plan at the Post Award Conference following the award of an order to the CO/COR for review and comment. The Contractor shall provide a final Project Plan to the CO/COR not later than 14 business days after the date of Post Award Conference.

2.8 INTELLECTUAL PROPERTY

IP rights will be governed by the applicable FAR clauses included in the BPA and as identified at the order level.

2.9 PROTECTION OF INFORMATION

The Government will provide all necessary information, data, and documents to the Contractor for work required under this BPA. The Contractor shall use Government furnished information, data, and documents only for the performance of work under this BPA 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 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).

References:

- DHS Management Directive 140-01, "*Information Technology System Security Program, Sensitive Systems"*
- DHS 4300A Policy Directive (Version 13.2, September 20, 2022).
- 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.

2.10 RECORDS MANAGEMENT OBLIGATIONS

The term Federal record:

1. Includes CISA records.
2. Does not include personal materials.
3. Applies to records created, received, or maintained by Contractors pursuant to their CISA BPA or order.
4. May include deliverables and documentation associated with deliverables.

Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the BPA and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

CISA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CISA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to CISA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the BPA and order. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to CISA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the BPA or each order. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this BPA requiring the disclosure of information, documentary material and/or records generated under, or relating to, BPAs. The Contractor (and any sub-contractor) is required to abide by Government and CISA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

The Contractor shall only use Government Information Technology (IT) equipment for purposes specifically tied to or authorized by the BPA and in accordance with CISA policy.

The Contractor shall not create or maintain any records containing any non-public CISA information that are not specifically tied to or authorized by the BPA.

The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

CISA owns the rights to all data and records produced as part of this BPA and subject orders. All deliverables under the BPA and orders are the property of the U.S. Government for which CISA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Deliverables shall incorporate best practices in accordance with the United States Digital Services Playbook standard (https://playbook.cio.gov) and be compliant with Section 508 (http://www.section508.gov). Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

2.10.1 RECORDS MANAGEMENT TRAINING

All Contractor employees assigned to this BPA who create, work with, or otherwise handle records are required to take CISA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

2.10.2 FLOW-DOWN OF REQUIREMENTS TO SUBCONTRACTORS

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this BPA, and require written subcontractor acknowledgment of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

3.0 DELIVERABLES

The Contractor shall consider items in **BOLD** as having mandatory due dates.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	SUBMITTED BY	DISTRIBUTION
1	**2.1.1**	**Transition-In Plan**	**Within 10 days after Kick Off meeting**	**Program Managers**	**CO, COR**
2	2.1.1	Staffing Plan	Submit with Transition-In Plan	Program Managers	CO, COR
3	2.1.2	Weekly Status Report	Monday, from the previous week by NLT 2:00 PM EST	Project Managers	COR
4	**2.1.3**	**Monthly Financial Report**	**25th of the month**	**Program Managers**	**COR**
5	**2.1.4**	**Organizational Charts**	**25th of the month**	**Program Managers**	**COR**
6	**2.1.5**	**Transition-Out Plan**	**120 days prior to BPA/Call Order expiration date**	**Program Managers**	**CO, COR**
7	**2.16**	**Business Continuity Plan**	**15 business days after the date of award; to be updated annually**	**Program Managers**	**CO, COR**
8	**2.1.9**	**Progress Reports**	**Monthly**	**Project Managers**	**CO, COR**
9	**2.6**	**Post Award Conference**	**14 business days after date of award**	**Program Managers**	**CO, COR**

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	SUBMITTED BY	DISTRIBUTION
10	**2.7**	**Project Plan**	**Draft due at Post Award Conference; final due 14 business days after Post Award Conference**	**Project Managers**	**CO, COR**
11	2.10	Progress Meetings	Upon request	Project Managers	CO or COR
12	4.3	Contractor Key Personnel	15 days in advance of change	Program Managers	CO, COR
13	6.2	Asset Management Report	25TH of the Month	Project Managers	COR
14	7.0	Invoices	Monthly	Contractor Financial Office	CO, COR

3.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The COR provides technical direction and guidance based on the requirements identified in this SOW. The COR works closely with the contractor's Program Manager and/or Project Manager to issue interpretations of technical requirements; to monitor the contractor's performance under the contract and notify the CO of any deficiencies observed. The COR will provide no supervision to contractor personnel. The COR is not empowered to make any commitments or changes which affect the contract price or other items and conditions. Any such proposed changes must be brought to the immediate attention of the CO for action. The acceptance of any changes by the contractor without specific approval and written consent of the CO shall be at the contractor's risk.

4.0 CONTRACTOR PERSONNEL

4.1 QUALIFIED PERSONNEL

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

4.2 CONTINUITY OF SUPPORT

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

4.3 CONTRACTOR KEY PERSONNEL

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the CO/COR no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace Key Contractor personnel without approval from the CO. Contractor Key personnel shall not be assigned by the Contractor to more than one key position for this requirement.

"Key Personnel" is defined as contractor personnel who are recognized by the Government and Contractor as essential to the successful completion and execution of this BPA or each order. Contractor shall provide resumes with the quote for Key Personnel. Contractor shall identify the following positions as key personnel and provide personnel with the qualifications below:

- Program Managers for BPA awardees – Each Contractor awardee shall identify a program manager to oversee the day-to-day operations of CISA DTSS and serve as the contractor's Point of Contact (POC) for the Contracting Officer Representative (COR), and senior level Government managers. Every BPA awardee shall have a Program Manager. The contractor Program Manager shall have the following qualifications:

    - Possess a Top Secret (TS) Clearance.
    - Required to be eligible to be granted aSensitive Compartmented Information (SCI) from DHS.
    - Project Management Professional (PMP) and ITIL v3 Foundation certified to ensure BPA functions, program/project management services, performance tracking and reporting, and BPA execution are conducted and managed according to industry best practices.
    - A minimum of seven (7) years of experience in IT program management.
    - A bachelor's degree in Management, computer science, or information systems.
    - Experience with applying the Agile and Scrum methodologies.

    The Program Manager shall be responsible for all Contractor work performed under this SOW. It is anticipated that the Program Manager shall be one of the senior level employees provided by the Contractor for this work effort. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the

absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this BPA. Additionally, the Contractor shall not replace the Program Manager without prior approval from the Contracting Officer.

The Program Manager shall be available to the COR via telephone between the hours of 0800 and 1600 ET, Monday through Friday, and shall respond with acknowledgement to a request for discussion or resolution of technical problems within 1 hour of notification. Discussion can be scheduled at a later date and time at the discretion of the government COR and government Program Manager.

- Project Manager for each order – The Contractor awardee shall provide a Project Manager who shall be responsible for providing centralized administration of all work performed under each order. The Project Manager shall be the single point of contact for the Contracting Officer and the COR and have the authority and responsibility to assign tasks and work elements; make business, product, and technical decisions; and be accountable for the success or failure of the overall service(s) under the order. This POC is ultimately responsible for how well the service meets needs of its users. The contractor Project Manager shall have the following qualifications:

    - Possess a Top Secret (TS) Clearance.
    - Required to be eligible to be granted aSensitive Compartmented Information (SCI) from DHS.
    - Project Management Professional (PMP) and ITIL v3 Foundation certified to ensure BPA functions, program/project management services, performance tracking and reporting, and BPA execution are conducted and managed according to industry best practices.
    - A minimum of five (5) years of experience in IT program management.
    - A bachelor’s degree in Management, computer science, or information systems.
    - Experience with applying the Agile and Scrum methodologies.

  The name of the Project Manager, and name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor’s quote for the order. During the absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Project Manager without prior approval from the Contracting Officer. The Project Manager shall be available to the COR via telephone or electronic means between normal business hours and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification.

The Project Manager shall be available to the COR via telephone between the hours of 0800 and 1600 ET, Monday through Friday, and shall respond with acknowledgement to a request for discussion or resolution of technical problems within 1 hour of notification. Discussion can be scheduled at a later date and time at the discretion of the government COR and government Project Manager.

4.4 CONTRACTOR TELECOMMUTING – REMOTE PERSONAL RESIDENCE WORK LOCATIONS

Telecommuting for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. 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. Telecommuting (Telework) is permitted under the order in accordance with the requirements below, with the approval of the Government Technical Lead and the COR.

Contractor's may propose work be performed at the Government's facility, Contractor's facility, or any combination thereof, to the extent that the Contractor can satisfy all information, personnel, and physical security requirements to perform the work without added cost or burden to the Government. All telework requests must be approved by the COR.

When contract support is authorized to be performed from a telework location such as the contractor facility or contractor's personal residence, the maximum level of access authorized is Unclassified FOUO. In addition, the contractor will ensure that information is not accessed by others who do not have a need-to-know. Teleworking for federal government contractors will be considered at the discretion of the COR, and on a situational basis to the extent practicable to meet DHS mission needs. Teleworking allows contractor personnel to perform their contractual requirements outside of the designated CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telework for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. Teleworking is permitted under the task order in accordance with the requirements below. All work performed outside of the above-mentioned DHS facilities will be performed at the Unclassified FOUO level. Access to Unclassified FOUO information and GFE will only be accessed from authorized CONUS locations. Information nor GFE is authorized to be taken or accessed from OCONUS locations. Measures must be initiated to prevent unauthorized access by personnel without a need-to-know from accessing Unclassified FOUO information when teleworking from contractor facility (s) and contractor's personal residence(s).

All telework that requires access to DHS Government Furnished Equipment (GFE), information, or remote systems must only be conducted in the Continental United States (CONUS) and U.S. Territories and some Outside CONUS (OCUNUS) locations such as Alaska and Hawaii. Any access or use of GFE, information or remote access OCONUS locations besides the ones listed

above, must be requested by the Government Program Manager (PM), and approved by the COR, after all requirements are met. Any OCONUS use or access, not authorized, will result in immediate revoking of all privileges and access to systems.

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

4.4.1 TELEWORK

A. Definitions

"Telework" is an alternative work arrangement which allows a contractor employee to perform work at an alternate worksite (e.g., home, telework center, contractor's office). In accordance with 41 U.S.C. § 3306(f), employees of Federal Government contractors are permitted to telework in the performance of contracts entered into with executive agencies. The term "telecommuting" used in the Federal Acquisition Regulation (FAR) is synonymous with the term "telework" as used in this clause. A contractor employee can telework on a core or episodic basis. A core arrangement occurs on a routine and recurring basis, whereas an episodic arrangement occurs on an occasional and non-routine basis, such as during inclement weather.

"Telework-ready contractor employee" is a contractor employee who has been approved to telework, has an established alternate worksite, is prepared to telework by having enough work to cover the scheduled telework period, and has the appropriate secure technology equipment to meet the needs of the telework arrangement and a high-speed Internet connection.

B. Requirements

The Contractor shall provide adequate oversight of work products when telework is authorized to ensure continuity of contract performance and quality control.

Equipment provided by CISA for telework purposes will be treated as GFE. All CISA training required for telework-ready contractor employees shall be completed prior to commencement of an individual's telework schedule. The Contracting Officer's Representative (COR) will notify the Contractor's program manager (PM) of the required training courses. Once the training is completed, contractor employees shall submit their certificates of completion to the COR. Contractor employees shall comply with the security requirements stated in HSAR 3004.470 and HSAM 3004.470 and work according to the guidance set forth in DHS 4300A, Sensitive Systems Handbook, Rules of Behavior (Version 13.2, September 20, 2022).

A contractor employee's telework schedule shall be approved by the Contractor's PM and coordinated with the COR. Once approved, requests to change a scheduled telework day shall be submitted in advance, when possible, to the Contractor's PM, who will coordinate with the COR.

The Contractor's PM continues to be responsible for contractor employees' time and attendance and notifying the COR of any changes.

If a Federal Government closing affects the Government facility, contractor employees who are telework-ready shall begin to telework at their normal start time and are expected to work the entire day. If OPM announces the option for unscheduled telework, a contractor employee may request to telework by contacting the Contractor's PM, who will coordinate with the COR.

If a contractor employee has performance issues, does not follow the security procedures, or does not complete required training while in a telework status, the COR will contact the Contractor's PM and the contractor employee's telework privileges may be revoked.

C. Information Technology (IT) and Security

Contractor employees are required to use only GFE provided by CISA when teleworking. Should the GFE fail or require repair or replacing, the contractor employee shall be required to return to the traditional worksite to perform their duties. CISA shall provide maintenance and technical support for IT GFE used by teleworkers. CISA's inability to provide IT GFE shall not constitute an excusable delay. The Contractor or contractor employee is responsible for providing high-speed internet connectivity for teleworking and will bear the cost of the internet connection. The contractor employee shall be accessible at all times, via telephone, e-mail, or video conferencing during his/her working hours.

Contractor employees' use of GFE and Government information shall be for contractual performance only and shall be protected from unauthorized access, disclosure, sharing, transmission, or loss. The contractor employee shall keep Government property and information safe, secure, and separated from his/her personal property and information. Contractor employees who telework shall be the sole operators of the GFE they use. Contractor employees who telework shall not work on, have access to, or keep in their possession classified information at an alternate worksite. Contractor employees shall comply with the guidance in the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.

Contractor employees shall return all GFE provided by CISA to the COR upon separation from the contract.

4.4.2 CONTRACTOR LABOR RATES CHARGED WHILE TELECOMMUTING

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

4.5 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules

and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and always display all identification and visitor badges in plain view above the waist.

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.

4.6 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 always present a professional appearance and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

4.8 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 individual order. 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

Contractor must possess and retain an active final Top-Secret facility security clearance (FCL) granted by the Defense Counterintelligence and Security Agency (DCSA) at the time of solicitation/proposal submission. DHS does not accept Interim FCLs.

Contractor BPA level Program Manager and order level Project Managers will require access to classified information at the Top-Secret level with elibility to obtain Sensitive Compartmental Information (SCI) during the performance of duties granted by DHS.

- Required to possess and retain a Top Secret (TS) Clearance.
- Required to be eligible to be granted a Sensitive Compartmented Information (SCI) by DHS.

All other contractor personnel will require access to Unclassified FOUO information.

Safeguarding of classified information at the contractor facility is not authorized. All access to classified information will be at the government location as specified in the place of performance. Access to classified information will be accessed solely from CISA facilities. The details will be specified in the Department of Defense Contract Security Classification Specification (DD Form 254).

Contractor access to CISA Sensitive Information, systems, networks, and reoccurring access to CISA facilities is required under this SOW; therefore, contractor employees will 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 (End of Definition). 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) When information is provided by the government to the contractor, information will be marked with the appropriate dissemination markings (FOUO/SBU, etc.).
(2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."

5.2 POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR BPA ORDERS

1. The procedures outlined below shall be followed for the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness determinations, as required, in a timely and efficient manner.

2. Carefully read the security clauses in the BPA. Compliance with the security clauses in the BPA is not optional.

3. Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the BPA and Call Order, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the Call Order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS OCSO/PSD. Prospective contractor employees shall submit the below completed forms to the DHS OCSO/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) days before the start date of the order or thirty (30) days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form (SF) 85-P, ―Questionnaire for Public Trust Positions‖
- SF-85P Certification
- SF-85P Authorization for Release of Information
- FD Form 258, ―Fingerprint Card (2 copies)
- 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

4. Only complete packages will be accepted by the DHS OCSO/PSD. Specific instructions on submission of packages will be provided upon award of the order.

5. The DHS OCSO/PSD may, as it deems appropriate, authorize, and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable Fitness determination will follow. In addition, a favorable EOD or Fitness 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 BPA. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or Fitness determination by the DHS OCSO/PSD.

6. Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a government employee and the purpose of the visit is to attend a limited number of required briefings or nonrecurring meetings to facilitate the transition of a BPA or order. The intent of this statement is to allow a minimum amount of meeting / transition attendances to prepare for the new BPA.

7. The DHS OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's 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 whom it was issued and the last known location and disposition of the pass or card.

6.0 GOVERNMENT FURNISHED RESOURCES

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

6.1 PROPERTY INVENTORY

Contractor shall establish and maintain an accurate master inventory of all property purchased for CISA under this BPA or individual orders.

6.2 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. The Contractor shall submit this report monthly to the COR by the 25th of every month. 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

7.0 INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per Attachment 5, Contract Clauses. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR 52.232-1 Payments, FAR 52.232-7, Payments under Time and Materials and Labor-Hours FAR 52.232-25 Prompt Payment, and. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS.
2) BPA Order Number.
3) Modification Number, if any.
4) UEI Number.
5) Month services provided
6) CLIN and Accounting Classifications
7) Contract Line-Item Number (CLIN) and description for each billed item.
8) Any additional backup information as required by this BPA.
9) ATTN: CISA/MBSO

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

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.

The contractor shall submit invoices monthly. The Contractor shall submit the invoice electronically to the address below:

CISAInvoice.Consolidation@ice.dhs.gov

Simultaneously copy the following individuals in the same email:

Contracting Specialist
Contracting Officer's Representative

8.0 GOVERNMENT ACCEPTANCE PERIOD

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

The CO 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 CO of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

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

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