Flexible Agile Scalable Teams (FAST) Blanket Purchase Agreement (BPA)

SECTION II – PERFORMANCE WORK STATEMENT (PWS)

1.0 PURPOSE

1.1 Product, Service, or Outcome Needed

The goal of the FAST BPA is to provide full service, enterprise-focused applications development capabilities where IT services are delivered through state-of-the-art, service-enabled IT software systems and dynamic computing environments. Through the scope of this BPA, the Office of Information Technology (OIT) shall provide portable, reusable, and interoperable business-driven solutions to support the greater mission of TSA.

The activities identified in the FAST BPA shall maintain a focus on the following key outcomes:

- Increase use and deployment of mobile applications.
- Decreased operations and maintenance support and cost.
- Reduction in the number of legacy applications through functionality consolidation.
- Increased standardization of operating systems and IT technologies/architecture.
- Increased use of SaaS/PaaS and microservices solutions.
- Improved analytics and business intelligence (BI) platform and data management capabilities that promotes self-service, increased agility, and provides faster insight.
- Increased automation of application delivery, testing, and data migration.
- Convert legacy applications to SaaS/PaaS.
- Reduced implementation cost by leveraging cloud services and capabilities.
- Adoption and integration of agile methodologies and practices across TSA.
- Create partnerships with industry leaders to capitalize on best practices and leading-edge solutions with emphasis on innovation and future ideation.

1.2 Scope of the Product, Service, or Outcome

In support of the mission needs of TSA and its stakeholders, the Information Technology (IT) provides excellence in the management, execution, and leadership of
TSA’s information technology needs. As part of this mission, OIT offers applications development and production support services for all TSA stakeholders. To enable these services, IT is establishing a contract vehicle that encompasses the following scope:

- **Applications Development Support**
  - Use of various development approaches for application implementation, delivery, development, and testing (predominately, employ Agile methodology, however, waterfall may be applied as organizations transition)
  - SaaS/PaaS implementation and support
  - Deploy and support COTS
  - Mobile
  - Backlog Grooming/Backlog Management
  - Code delivery using automation tool
  - Continuous Integration/Continuous Delivery (CI/CD)
  - DevOps and DevSecOps
  - Deployment activities (e.g., release management)
  - Data migration
  - Accessibility (Section 508) testing

- **Applications Production Support**
  - Level 2 and 3
  - Decommission applications or systems
  - Triage and report issues

- **After Hours/Emergency Support**

- **Program Management Support**
  - Discovery and requirements management
  - Plan and conduct demonstrations

- **Subject Matter and Senior Technology Expertise Support**
  - UI/UX and Design Thinking Expertise
  - Agile Transformation and Change Management Support
  - Information Assurance Expertise

- **Architecture/Platform Evolution Support**

- **Continuous Process Improvement**

- **Operations Engineering/Operations & Maintenance (O&M)**

- **Systems Engineering**

- **Environment Management**

- **Continuity of Operations (COOP)**
2.0 BACKGROUND

The Transportation Security Administration (TSA) protects the Nation’s transportation system to ensure freedom of movement for people and commerce. To support this mission, the TSA Office of Information Technology (OIT) ensures the security, integrity, and productivity of TSA and its employees through Information Technology (IT) capabilities. In order to successfully execute this mission, TSA must have the capability to customize mission support systems, develop custom software solutions when no solution is commercially available or from Government sources. TSA plans to leverage more commercial, out-of-the-box (OOTB)/Commercial Off-the-Shelf (COTS), Software-as-a-Service/Platform-as-a-Service (SaaS/PaaS) solutions that enable mission capabilities at a lower cost.

TSA customers require a full range of system and application design, agile software development, and application production support services. To achieve integration and customization of mission support systems and applications, TSA needs multiple Agile teams in support of Agile design, development, testing, and adaptive maintenance activities. TSA is moving towards operations and maintenance (O&M) being part of the agile development lifecycle in other words an approach that promotes the idea, “if you build it, you own it”. The objective of the TSA Flexible Agile Scalable Teams (FAST) procurement is to establish an OIT contract vehicle that supports Agile design, development, and application production requirements for a suite of applications that support the entire agency.

TSA Application Development Division (ADD) is moving towards modern architecture standards and delivery practices, like microservices, continuous integration and deployment, automated testing, and leveraging the cloud. These approaches allow for small teams to deliver the business value without requiring a scaling framework.

In 2013, TSA awarded Operational Applications Support and Information Services (OASIS) II as a BPA on the GSA IT Schedule 70. The purpose of OASIS II was to provide a custom software development capability that leads the way to innovation and IT excellence. The FAST contractor(s) shall continue the established TSA applications development program and shall serve as a source of innovation and transformation.

3.0 TECHNICAL REQUIREMENTS/TASKS/OUTCOMES

TSA requires a highly qualified and capable contractor whose members:

- Provide applications development services, in multiple hardware/software environments that span a wide range of requirements. These required development services also include multiple development methodologies.
- Enable, by system design, adoption of cloud computing services in different cloud models including Public, Private, Hybrid, and Community models.
- Provide services and support in administering such managed services for cloud computing, including but not limited to overall management, billing, quality control, dispute resolution, and rate optimization as required.
- The ability to obtain public and subscription-based information (i.e. automated data
feeds from external sources such as FAA flight delay data, DHS procurement approval status data and Coast Guard financial data) on demand and present it in informative and innovative ways to the public and TSA staff, as directed.

- Consult and collaborate with TSA and other stakeholder program officials on all required services and applications.
- Apply various IT Software Systems Development and Support approaches to different scenarios, unique requirements, and desired system behaviors through required labor categories and relevant skill sets.
- Demonstrate the understanding, knowledge, and ability to accomplish the IT software systems development and support critical to the vision of TSA and its efforts to create an enterprise that is responsive to dynamic mission requirements.
- Ability to work in the diverse environments at TSA.
- Demonstrate ability to comprehend the requirements and provide the appropriate knowledgeable and experienced staff.
- Demonstrate knowledge in utilization of cloud-based computing services.
- Provide innovative ideas to reduce application development costs.

3.1 Applications Development

- The contractor(s) shall develop applications in accordance with the DHS Software Engineering Lifecycle (SELC). Within the context of the SELC framework, the contractor shall use a variety of development approaches and methodologies; for example: Agile including Scaled Agile Framework (SAFe) and Waterfall.
- Overall the general applications are web interfaces using Oracle database, Oracle Business suite, Java, .net, DB2, Microsoft SQL Server, and Microsoft SharePoint.
- Currently there are about 15-25 custom applications on the release schedule at TSA. There are about 95 custom applications of which approximately 15 are large enterprise applications. Approximately 200-250 application releases were deployed to production in the last 12 months when including versions, releases and maintenance.
- The contractor(s) shall design, develop, and enhance applications as requirements emerge/evolve. The vendor working with government will determine team makeup depending on development project, e.g., COTS, custom application, SaaS/PaaS, etc. Through the continuous discovery process, additional teams or team members, may be added to development teams, as new requirements become known.
- The contractor shall provide in-depth knowledge of the supported applications in order to perform enhancements that have been identified by the product owner and placed in the backlog, for example, defects found from the application production support team.
- The contractor(s) shall provide OIT and its customers with experienced, cross-functional development teams. Agile teams should be designed to be high performing autonomous teams with enough flexibility to work across multiple technology stacks. Team members shall have “T-shaped” skills, meaning that they have significant skill depth in a few specific areas, but have broad skills across multiple capability areas that allow them to contribute more generally across multiple areas. All team members shall have at least some level of programming knowledge. The teams shall deliver viable solutions in support of TSA’s
strategic mission and objectives.

- The contractor(s) shall perform the full suite of development tasks using Agile methodologies, including, but not limited to: User story collaboration, backlog grooming/backlog management, defining done and acceptance criteria, user centered design, code development, integration support, automated testing, usability testing (including accessibility 508 and Security tests), DevOps (including CI/CD), configuration management/change control, data operations, deployment activities (e.g., release management), and user training.

- The contractor(s) shall deliver program increments from development to production. Delivery of working code into production with each program increment followed by a system increment to support a system demo. Support the solution increment to collaboratively deliver the capability that is integrated, verified, and validated to meet both the functional and nonfunctional stories (requirements) in support of the Solution Demo.

- The contractor(s) shall perform data migration to include extraction, cleansing, database refactoring, and verification of data as applications are moved from on-premises to cloud IaaS, SaaS/PaaS solutions.

3.2 Applications Production Support

- The contractor(s) shall be a separate, independent, scalable team that is responsible for triaging and resolving Level 2 and 3 incidents. Any incidents determined by the Product Owner resulting in application enhancements can be allocated to the agile development teams’ backlog. The application production support team shall receive application support requests from TSA’s Level 1 help desk (e.g., TSA SPOC (Single Point of Contact), other helpdesks, and other approved intake methods). The team shall provide support services to triage and resolve technical issues for TSA software application and enterprise middleware.

- The contractor(s) shall decommission designated or obsolete applications or systems.

- The contractor(s) shall monitor applications and report system issues in a way that enables them to be systematically recorded, prioritized, solved, and tracked to closure and determine the cause of system issues and document the results of the analysis.

3.3 Program Management Support

- The contractor(s) shall manage all contractor resources and supervise all contractor staff in the performance of work on this contract in alignment with Management Plan. The contractor shall ensure each team member has experience and skills according to the proposed LCAT and their roles on the Agile team (e.g. software developer, scrum master, etc.). The contractor shall provide a Management Plan which will be used by the Government to ensure the proposed labor categories and experience are delivered. In the Management Plan, the contractor shall address the transition process and timing as new Agile teams are funded and on-boarded.

- The contractor(s) shall provide a comprehensive Staffing Plan that clearly defines all resources required to perform the activities and fulfill the responsibilities to provide the full range of IT services required to plan, manage, architect, engineer, develop, configure, test, and sustain the mission system. The Staffing Plan should detail how to accomplish the following: provide well qualified personnel; creating a stable workforce environment to develop high-performing teams, minimize learning curves and retain corporate knowledge;
develop a process and capability to quickly on-board/off-board and/or realign personnel in response to changing workloads or to respond to new or technically challenging assignments; maintain a 95% staffing level throughout the contract period of performance by maintaining a ready pool of cleared and qualified resources.

- The contractor(s) shall provide a resource-loaded Contractor Work Breakdown Structure (CWBS) outlining the proposed activities, resources and costs to complete the requirements in each TO. The CWBS shall align seamlessly into, and reflect the respective work outlined in the Government-provided Integrated Master Schedule (IMS).

- The contractor(s) shall coordinate with government to determine appropriate team size and composition as new requirements/projects are identified and approved.

- The contractor(s) shall conduct requirements management, including, working with customers and stakeholders, developing system domain knowledge, document requirements (e.g., mission, business, system, functional, performance, etc.), manage supporting documentation (e.g., ICDs), and manage requirements processes (e.g., submission, approval, etc.).

- The contractor(s) shall conduct system demos of system functionality each program increment.

3.4 Subject Matter and Senior Technology Expertise Support

- The contractor(s) shall provide senior technical expertise to mentor the agile development teams on skills required to deliver mission value. These experts communicate the program mission at the individual level, serve as advocates for the agile teams, and work closely with FAST leadership. They are involved in making centralized strategic decisions.

- The contractor(s) shall provide UI/UX design thinking expertise (e.g., apply Design Thinking, take a cloud first, mobile first, SaaS/PaaS first approach, design shared solutions, and provide input and recommendations for development of new applications).

- The contractor(s) shall demonstrate full understanding of agile methodologies and perform standard Agile Transformation and Change Management enablement activities.

- The contractor(s) shall demonstrate full understanding of Kanban and other methodologies for O&M support activities.

- The contractor(s) shall provide information assurance expertise.

3.5 Enterprise Architecture/Platform Evolution Support

- The contractor(s) shall ensure that all solutions and services meet DHS and TSA Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the Contractor shall comply with Homeland Security Enterprise Architecture (HLS EA) requirements.

- The contractor(s) shall continue to update tools, technologies, and environments to strengthen and evolve the architecture and technical platform of supported systems including: develop and maintain a cohesive Technology Roadmap; stay current with COTS software versions/releases/patches, refresh hardware and software well ahead of end-of-life and/or end-of-support; adopt open standard/open source/open architecture solutions; select and
implement DevOps tools and processes; adopt container architecture; assess opportunities and approaches for migration to cloud computing; identify and recommend options for significantly improving the current automated vetting tools; and identify and recommend options for significantly improving current data analytics.

- The contractor(s) shall comply with the following: DHS EA and associated reference models; TSA Segment and Solution architectures; TSA reference architectures; Homeland Security Presidential Directive (HSPD) 12; and Federal Information Protection Standard (FIPS) 201.

- The contract(s) shall assist the government in adding Technology Insertions into the DHS Technical Reference Model (TRM) and TSA Technology Solutions Portfolio (TechSP) and in submitting data assets, information exchanges, and data standards to the DHS Enterprise Data Reference Model.

3.6 Continuous Process Improvement Planning

The contractor(s) shall identify improvements to their daily work through continual learning and experimentation. Discoveries, both successes and failures, shall be documented and communicated. This will allow the rest of the team to avoid repeating failed experiments, and will promote the adoption and/or expansion of successful improvements across the organization.

3.7 Operations Engineering/Operations & Maintenance (O&M)

- The contractor(s) shall provide design, engineering, and integration support for all additions or changes to the infrastructure, particularly with respect to applicable applications (does not include applications covered under IMPACT contract), tools, and technologies used to manage, monitor, secure, and support system operations. In addition, ensuring the security of the system including implementing development and delivery processes that eliminate cybersecurity vulnerabilities and other system defects.

- The contractor(s) shall provide day to day operations and maintenance work to include, but not limited to, scheduled and unscheduled maintenance, recovery operations, backup and recovery deliverables, storage and media management, data archival and retention services, database administrative support, asset management, electronic drawing maintenance and deliverables, configuration management, infrastructure system sustainment and support, system monitoring and deliverables and mandatory Sabre development and support, in a multi-site configuration. Does not pertain to applications covered under IMPACT contract.

3.8 Systems Engineering

The contractor shall provide systems engineering support to include, but not limited to, planning and analysis; design of hardware and software solutions that integrate assets; application of technology to systems; system/application integration for improving/ensuring interoperability; trade-off analysis; development and enhancement of interfaces; application and data conversion; and system/subsystem level testing.

3.9 Environment Management

The contractor(s) shall maintain the configuration of the non-production environments.

3.10 Continuity of Operations (COOP)
The contractor(s) shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations may be disrupted and thus require activation of the CP and/or COOP. The contractor’s CP/COOP responsibility relates only to the system they provide or operate under contract.

3.11 Help Desk

The contractor(s) shall provide help desk support on a 24x7x365 basis to facilitate the resolution of technical issues that may arise from the user community, coordinate resolution of an average of 600 tickets on a monthly basis for all TSA personnel and operating locations for assistance with applications, and resolve technical issues and prioritize resolution, accordingly, to prevent critical problems and to ensure normal day-to-day operational activities can be completed.

3.12 After Hours Support

The contractor(s) shall provide support during normal business hours on weekdays, Saturdays, Sundays and Holidays: The support is for applications at “Severity Level 1 – System Down” or a problem as determined by the COR that requires immediate attention, such as end user assistance during an emergency event. The on-call Contractor resources must be available within 15 minutes to support the issue once contacted.

3.13 Innovation

TSA’s goal is to create a “cutting edge” technology organization. The solutions provided by the contractor(s) are expected to be comparable to the best systems, architectures, and approaches available in the private sector and beyond. The contractor(s) shall act as a change agent and trusted partner in building future-proof information technology capabilities that can rise to the challenge of the evolving counterterrorism mission. The contractor(s) must, through corporate experience and specific recommendations, demonstrate the capability to lead TSA’s technology innovations.

SECTION IV: General Requirements

A. Special Delivery Instructions:

All deliverables shall be created in the Department of Homeland Security Systems Engineering Life Cycle (DHS SELC) format whenever an applicable DHS SELC template is available.

Deliverables shall be provided to the Government Project Manager (GPM) and Contracting Officer’s Representative (COR) and shall be one soft copy via designated collaborative site in MS Office format clearly marked with:

- Title of the submittal
- DHS contract number
- TSA work order number, and
- CLIN

The contractor is hereby notified that TSA is a Microsoft based environment for office productivity tools.
Document deliveries must be in a Microsoft format (where applicable). ADD is continuing to evolve its application development process and practices including the adoption of new technologies to enhance the management of applications development efforts.

**B. Performance/ Delivery Period / Contract Type:**

**Period of Performance:**
- 12-month Base Period
- 12-month Option Year 1
- 12-month Option Year 2
- 12-month Option Year 3
- 12-month Option Year 4
- 12-month Option Year 5
- 12-month Option Year 6

**Contract Type:** Firm Fixed Price, Time and Material, and Cost Reimbursable (ODC’s)

**C. Place/ Location of Performance/ Delivery**

1. Specified work (e.g. meetings, presentations etc) on this procurement shall be detailed on each individual task order.

2. Local commuting expenses within a fifty (50) mile radius of the TSA Headquarters (currently in or near 601 12th Street, Arlington, VA) and other direct costs (cell phone, etc.) will not be charged to the Government.

**D. Accessibility Requirements (Section 508)**

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

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

**Section 508 Applicable EIT Accessibility Standards**

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement.
When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

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 COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available which meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section
508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@hq.dhs.gov.

**E. DHS and TSA Enterprise Architecture Compliance**

a) The Contractor shall ensure that all solutions, products, deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the Federal Enterprise Architecture Framework (OMB Reference Models).

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

   i. All developed solutions and requirements shall be compliant with the HLS EA.

   ii. The contractor shall align all solutions and services and ensure compliance with applicable TSA and DHS IT Security, Application, System, Network, Data, Information, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.

   iii. The contractor shall utilize any existing TSA or DHS user interface design standards, style guides, and/or policies and standards for human factors, usability, user experience, or human computer interaction (HCI).

   iv. All solution architectures and services (Application, System, Network, Security, Information, etc.) shall be reviewed and approved by TSA EA as part of the TSA SELC review process and in accordance with all applicable DHS and TSA IT governance policies, directives, and processes (i.e. TSA IT Governance Management Directive 1400.20). This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. All implementations shall follow the approved solution architecture/design without deviation. Any changes, to either the prior approved solution and/or prior approved design that are identified during subsequent SELC phases, including testing, implementation and deployment, shall undergo additional EA review prior to proceeding.

   v. All IT hardware and software shall be compliant with the TSA and HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to TSA and DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the TSA and HLS EA TRM Standards and Products Profile.

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

i. 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 and TSA data management architectural guidelines and subject to the TSA Enterprise Architecture Data Management Team (EDM) approval.

ii. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – ‘Rights in Data and Copyrights’ and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in an understandable format to TSA. Examples of data structures can be defined as, but not limited to

   a. Data models depicting relationship mapping and, or linkages
   b. Metadata information to define data definitions
   c. Detailed data formats, type, and size
   d. Delineations of the referential integrity (e.g., primary key/foreign key) of data schemas, structures, and or taxonomies

iii. All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within the ‘Requirements for Handling Sensitive, Classified, and/or Proprietary Information’, section of this SOW. This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system. Alternative data delivery techniques may also be defined by TSA Enterprise Data Management (EDM) team.

iv. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g. metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered in a TSA approved manner). Metadata shall also provide an indication of historical verses the most current data to be used, as well as frequency of data refreshes.

v. The contractor shall adhere to providing a Data Management Plan (DMP), as defined by Enterprise Architecture, to the EA design review team before the preliminary/critical design review. The Data Management Plan includes conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project’s data. All data artifacts must adhere to TSA EA data standards defined and published before the design review. Data Standards include but are not limited to, data asset standards, metadata standards, logical/physical naming standards, and information exchange (using
the National Information Exchange Model (NIEM)) standards. All required artifacts must be provided to and approved by the EA Design Review team.

d) 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.

F. Monthly Burn Report

On a monthly basis, contractors shall provide a monthly cost report to the GPM and COR for all non-fixed price contracts / work orders. The report will be designed to provide the government an accurate report for monthly contract expenses. This monthly report shall be within 5% of the actual monthly total cost. The report must address the following: (1) projected monthly cost vs actual monthly cost; (2) projected hours burned per labor category per CLIN vs actual hours burned per labor category per CLIN; (3) projected level of effort per task vs actual level of effort per task (as requested by GPM); (4) overall CLIN burn percentage; (5) overall contractual burn percentage. The report format shall include resource name, tasking, labor category, hourly labor cost, hours, and total cost matching the following format:

The Monthly Burn Report is required on the 15th of each month for the previous month’s burn rate. (If the 15th falls on a weekend/holiday, then the first business day prior to the 15th).

G. Transition Support

At the completion of performance of this task order, the contractor shall fully support the transition of the work identified to be transitioned to another entity, either government or a successor offeror(s). The contractor shall assist with transition planning and shall comply with established milestones and schedules of events.

The contractor shall be responsible for the transition of all technical activities identified in this task order. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all 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 analysis & design in process
- Certification that all non-public DHS information has been purged from any contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management team

If the government provides a Transition Plan template, the contractor shall complete this template as assigned, otherwise the contractor shall submit a Transition Plan at the direction of the government. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- 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

A Transition Plan shall be delivered 30 calendar days prior to the task order expiration date or, if directed by the government, 30 days prior to the end of each option period. The Transition Plan shall include support activities for all transition efforts for follow-on requirements to minimize disruption of services. The contractor shall account for a 10-business day Government review process prior to transition execution. The 10-day review and approval process is not included in the 30-day transition activities.

Transition support shall commence 30 business days prior to expiration of the Task Order. Upon award of a follow-on contract, the incumbent contractor will work with the new contractor to provide knowledge transfer and transition support, as required by the COR and PM.

**SECTION V: Information Assurance Requirements for TSA Government Acquisitions**

**Information Assurance Requirements for TSA Government**

FAST BPA PWS 14
Acquisitions (April 2016)

A. General Security Requirements

A.1. The Contractor shall comply with all Federal, Department of Homeland Security (DHS) and Transportation Security Administration (TSA) security and privacy guidelines in effect at the time of the award of the contract, as well as those requirements that may be discretely added during the contract.

A.2. The Contractor shall perform periodic reviews to ensure compliance with all information security and privacy requirements.

A.3. The Contractor shall comply with all DHS and TSA security controls to ensure that the Government’s security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 standards.

A.4. The Contractor shall include this guidance in all subcontracts at any tier where the subcontractor is performing the work defined in this statement of work (SOW).

A.5. The Contractor shall ensure all staff have the required level of security clearance commensurate with the sensitivity of the information being accessed, stored, processed, transmitted or otherwise handled by the System or required to perform the work stipulated by the contract. At a minimum, all Contractor staff shall be subjected to a Public Trust background check and be granted a Public Trust clearance before access to the System or other TSA resources is granted.

A.6. The Contractor shall sign a DHS Non-Disclosure Agreement (NDA) within (30) calendar days of the contract start date.

A.7. The Contractor shall not release, publish, or disclose agency information to unauthorized personnel, and shall protect such information in accordance with the provisions of the pertinent laws and regulations governing the confidentiality of sensitive information.

A.8. The Contractor shall ensure that its staff follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel shall be responsible for the physical security of their area and government furnished equipment (GFE) issued to the contractor under the terms of the contract.

A.9. The Contractor shall make all system information and documentation produced in support of the contract available to TSA upon request.

B. Training Requirements
B.1. All Contractor employees, requiring system access, shall receive initial Organizational Security Fundamentals Training within 60 days of assignment to the contract via the Online Learning Center (OLC). Refresher training shall be completed annually thereafter.

B.2. The Contractor shall complete annual online training for Organizational Security Fundamentals and TSA Privacy training.

B.3. Role Based training is required for contract employees with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, and shall be in accordance with DHS and TSA policy. The contractor will be notified if they have a position with significant security responsibility.

B.4. Individuals with SSR shall have a documented individual training and education plan, which shall ensure currency with position skills requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan shall be refreshed annually or immediately after a change in the individual’s position description requirements.

B.5. Information Security and Privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

B.6. The Contractor shall maintain a list of all employees who have completed training and shall submit this list to the contracting officer representative (COR) upon request, or during DHS/TSA onsite validation visits performed on a periodic basis.

B.7. The contractor shall its employees review and sign the TSA Form 1403 Computer and Wireless Mobile Device Access Agreement (CAA) prior to accessing IT systems.

C. Configuration Management (hardware/software)

C.1. Hardware or software configuration changes shall be in accordance with the DHS Information Security Performance Plan (current year and any updates thereafter), the DHS Continuous Diagnostics and Mitigation (CDM) Program to include dashboard reporting requirements and TSA’s Configuration Management policy. The TSA Chief Information Security Officer (CISO)/Information Assurance and Cyber Security Division (IAD) shall be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD POC shall approve any request for change prior to any development activity occurring for that change and shall define the security requirements for the requested change. The COR will provide access to the DHS Information Security Performance Plan.

C.2. The Contractor shall ensure all application or configuration patches and/or Requests for Change (RFC) have approval by the Technical Discussion Forum (TDF), Systems Configuration Control Board (SCCB) and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 Information Technology Security and TSA Information Assurance (IA) Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA CISO, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

C.3. The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.
C.4. The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting “sensitive information”) shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/NIST, National Information Assurance Partnership (NIAP) Evaluation and Validation Program.

C.5. US Government Configuration Baseline and DHS Configuration Guidance

a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB) and in accordance with DHS and TSA guidance.

1. USGCB Guidelines:

2. DHS Sensitive Systems Configuration Guidance

b) The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology shall also use the Windows Installer Service for installation to the default “program files” directory and shall be able to discretely install and uninstall.

c) Applications designed for general end users shall run in the general user context without elevated system administration privileges.

C.6. The Contractor shall establish processes and procedures for continuous monitoring of Contractor systems that contain TSA data/information by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). The Contractor shall perform monthly security scans on servers that contain TSA data, and shall send monthly scan results to the TSA IAD.

D. Risk Management Framework

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

D.1. The Security Authorization and Ongoing Authorization Process in accordance with NIST SP 800-37 and SP 800-137 (current versions) is a requirement for all TSA IT systems, including General Support Systems (e.g., standard TSA desktop, general network infrastructure, electronic mail), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework (RMF). Ongoing Authorization is part of Step 6 “Monitoring” of the RMF. All NIST guidance is publicly
available; TSA and DHS security policy is disclosed upon contract award with some exceptions, which are public facing (i.e., [DHS Security and Training Requirements for Contractors](#)).

D.2. A written Authorization to Operate (ATO) granted by the TSA Authorizing Official (AO) also known as TSA Chief Information Security Officer (CISO) is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.


D.4. Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation shall be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

D.5. The Security Authorization (SA) Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation: 1) Security Assessment Report (SAR), 2) Security Plan (SP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Security Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Assessment Plan (SAP), 9) Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Ongoing Authorization Artifacts as required by the DHS Ongoing Authorization Methodology (current version). The SA package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents shall be reviewed and approved by the CISO and the IAD, and accepted by the CO upon creation and after any subsequent changes, before they go into effect. Ongoing Authorization artifacts include monthly TRigger Accountability Log (TRAL), monthly operating system scan results, application scans as directed, updated control allocation table (CAT), and associated memos as directed. All steps in the DHS Information Assurance Compliance Systems (IACS) shall be completed correctly, thoroughly and in a timely manner for all steps of the RMF.

D.6. The contractor shall support the successful remediation of all identified system weaknesses and vulnerabilities that are identified as a result of the aforementioned security review process.

D.7. The contractor shall submit and analyze monthly operating system vulnerability scans for the DHS Information Security Performance Plan FISMA Scorecard. Vulnerabilities not remediated are generated into Plan of Action and Milestone (POA&M)s after 30 days.

E. Contingency Planning

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)
E.1. The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations may be disrupted and thus require activation of the CP and/or COOP. are disrupted. The contractor’s CP/COOP responsibility relates only to the system they provide or operate under contract.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in the DHS IACS Tool. If access has not been provided initially, the contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K IT Contingency Plan Template.

E.3. The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

E.4. The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

E.5. The Contractor shall test their CP annually and retain records of the annual CP testing for review during periodic audits.

E.6. The Contractor shall record, track, and correct any CP deficiency; any deficiency correction that cannot be accomplished within one month of the annual test shall be elevated to IAD.

E.7. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.8. The Contractor shall have an Emergency Response Plan that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other incident or activity that may endanger lives, property, or the capability to perform essential functions.

E.9. The Contractor shall have a Backup Operations Plan that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason.

E.10. The Contractor shall have a Post-disaster Recovery Plan that includes procedures and responsibilities to facilitate rapid restoration of normal operations at the primary site or, if necessary, at a new facility following the destruction, major damage, or other major interruption at the primary site.

E.11. The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

E.12. The Contractor shall ensure a full backup of all network data occurs as required by the system’s availability security categorization impact rating per TSA Information Assurance policy.

E.13. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) shall be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one hour.

E.14. The Contractor shall ensure sufficient backup data to facilitate a full operational recovery within one business day at either the prime operational site or the designated alternate site shall be stored at a secondary location determined by the local element disaster recovery plan.
E.15. The Contractor shall ensure that data at the secondary location is current as required by the system’s availability security categorization impact rating.

E.16. The Contractor shall ensure the location of the local backup repository and the secondary backup repository is clearly defined, and access controlled as an Information Security Restricted Area (ISRA).

E.17. The Contractor shall adhere to the DHS IT Security Architecture Guidance Volume 1: *Network and System Infrastructure* for the layout of the file systems, or partitions, on a system’s hard disk impacting the security of the data on the resultant system. File system design shall:

- Separate generalized data from operating system (OS) files
- Compartmentalize differing data types
- Restrict dynamic, growing log files or audit trails from crowding other data

E.18. The contractor shall adhere to the DHS IT Security Architecture Guidance Volume 1: *Network and System Infrastructure* for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

F. Program Performance

F.1. The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the Contracting Officer (CO).

F.2. The Contractor shall provide support during the IAD audit activities and efforts. These audit activities shall include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

F.3. Upon completion of monthly security scans, findings shall be documented and categorized as High, Moderate, or Low based on their potential impact to the System IT Security posture. The Contractor shall provide TSA with estimates of the total engineering service hours required to support the remediation of open POA&M items. High security findings shall be remediated first in 45 days or less; Moderate security findings shall be remediated in 60 days or less, and Low security findings shall be remediated in 90 days or less. The Contractor shall work with the TSA System ISSO and the respective CO and/or Contracting Officer’s Representative (COR), as well as OIT IAD and the System Owner (as required) to prioritize and plan for the remediation of open POA&Ms. The TSA System ISSO shall maintain all security artifacts and perform Ongoing Authorization (per NIST 800-137 and DHS-TSA requirements) and Continuous Diagnostics and Mitigation (CDM) (per OMB M-14-03) activities to ensure active compliance with security requirements. Specific POA&M guidance and information can be found in the SOP 1401 *Plan of Action and Milestone (POA&M) Process*, as well as the DHS 4300A PD Attachment H *Plan of Action and Milestones (POA&M) Process Guide*.

G. Federal Risk and Authorization Management Program (FedRAMP)

If a vendor is to host a system with a Cloud Service Provider, the following shall apply:
G.1. **FedRAMP Requirements:** Private sector solutions shall be hosted by a Joint Authorization Board (JAB)-approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) ([http://cloud.cio.gov/fedramp/cloud-systems](http://cloud.cio.gov/fedramp/cloud-systems)) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The CSP shall adhere to the following in addition to the FedRAMP requirements:

- Identity and entitlement access management shall be done through Federated Identity;
- SSI and PII shall be encrypted in storage and in transit as it is dispersed across the cloud;
- Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS or SaaS levels;
- Cloud bursting shall not occur;
- TSA data shall be logically separated from other cloud tenants;
- All system administrators shall be properly cleared and vetted U.S. citizens;
- TSA data shall not leave the United States; and

- The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has EINSTEIN 3 Accelerated (E3A) capabilities deployed. These include but are not limited to the analysis of network flow records, detecting and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The E3A capability shall use the Domain Name Server Sinkholing capability and email filtering capability allowing scans to occur destined for .gov networks for malicious attachments, Uniform Resource Locators and other forms of malware before being delivered to .gov end-users.

G.2. **Private Sector System Requirements:** TSA shall conduct audits at any time on private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS IACS. The private sector systems are required to go through the Security Authorization Process and the RMF in accordance the Federal Information Systems Management Act (FISMA) and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has E3A deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Management Directive 1400.3 and its Attachment 1 (TSA IA Handbook) shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS and communicated by the contracting officer representative (COR) or contract security point of contact (POC).

H. **Information Assurance Policy**

H.1. All services, hardware and/or software provided under this task order shall be compliant with applicable DHS 4300A Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook,
TSA MD 1400.3 Information Technology Security, TSA IA Handbook, Technical Standards (TSs) and standard operating procedures (SOPs).

H.2. The contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which shall be provided by the Contracting Officer.

H.3. Authorized access and use of TSA IT systems and resources shall be in accordance with the TSA IA Handbook.

H.4. The contractor shall complete TSA Form 251 and TSA Form 251-1 for sensitive or accountable property. The contractor shall email the completed forms to TSA-Property@dhs.gov and include a hard copy with the shipment.

I. Data Stored/Processed at Contractor Site

I.1. Unless otherwise directed by TSA, any storage of data shall be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

J. Remote Access

J.1. The Contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct sanctioned TSA business. Therefore, remote access rights shall be expressly granted, in writing, by the TSA IAD.

J.2. The Contractor employee(s) remote access connection to TSA networks shall be terminated immediately for unauthorized use, at the sole discretion of TSA.

J.3. The Contractor shall use his or her federal issued personal identifiable verification (PIV) badge to access TSA resources to include IT applications and physical facility.

K. Interconnection Security Agreement

If the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity, the following shall apply:

K.1. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented using an interagency agreements; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

K.2. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

K.3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

L. SBU Data Privacy and Protection

This section is not applicable if contract has DHS Sensitive Information Required Special Contract

FAST BPA PWS 22
Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

L.1. The contractor shall satisfy requirements to work with and safeguard Sensitive Security Information (SSI), Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (Sensitive PII). All support personnel shall understand and rigorously follow DHS and TSA requirements, SSI Policies and Procedures Handbook, and Privacy policies, and procedures for safeguarding SSI, PII and SPII.

L.2. The contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor’s control. All TSA data, including but not limited to PII, SPII, Sensitive Security Information (SSI), Sensitive But Unclassified (SBU), and Critical Infrastructure Information (CII), shall be protected according to DHS and TSA security policies and mandates.

L.3. TSA shall identify IT systems transmitting unclassified/SSI information that shall require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

- FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2 (current version)
- National Security Agency (NSA) Type 2 or Type 1 encryption (current version)
- Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the DHS 4300A Sensitive Systems Handbook), current version

L.4. The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII shall comply with TSA MD 3700.4, Handling Sensitive Personally Identifiable Information (current version).

L.5. Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA IA Handbook, and applicable IT Security Technical Standards and SOPs.

L.6. The contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA IA Handbook, applicable Technical Standards, SOPs and TSA MD 3700.4, Handling Sensitive Personally Identifiable Information.

L.7. The Contractor shall ensure that source code is protected from unauthorized access or dissemination (see TSA IA Handbook).

M. Disposition of Government Resources

M.1 At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA IA
The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, TSA Technical Standard 046 IT Media Sanitization and Disposition, and SOP 1400-503 IT Media Sanitization. The contractor shall email a signed, by the contractor’s designated security officer or senior official, proof of sanitization to the COR. In addition, the contractor shall provide the contracting officer a master asset inventory list that reflects all assets, government furnished equipment (GFE) or authorized non-GFE that were used to process TSA information.

N. Special Considerations and Circumstances (if applicable and when requested)

N.1 For major agency Information Technology (IT) infrastructure support ranging in the total estimated procurement value (TEPV) of about $100 million or above or per TSA management’s request, the contractor shall provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA IAD. This plan shall describe the processes and procedures that shall be followed to ensure the appropriate security of IT resources are developed, processed, or used under this contract. At a minimum, the contractor’s SPP shall address the contractor’s compliance with the controls described in NIST SP 800-53 (current version). The security controls contained in the plan shall meet the requirements listed in the TSA IA Handbook, Technical Standards and the DHS Sensitive Systems Policy Directive and Handbook 4300A (current versions).

N.2 The SPP shall be a living document. It shall be reviewed and updated semi-annually, beginning on the effective date of the contract, to address new processes, procedures, technical or federally mandated security controls and other contract requirement modifications or additions that affect the security of IT resources under contract.

N.3 The SPP shall be submitted within 30 days after contract award. The SPP shall be consistent with and further details the approach contained in the offeror’s proposal or quote that resulted in the award of this contract and in compliance with the system security requirements.

N.4 The SPP, as submitted to the Contracting Officer, and accepted by the Information Systems Security Officer (ISSO), shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

O. Trusted Internet Connection 2.0 Requirements for Managed Trusted Internet Protocol Service Offering (MTIPS)

O.1 MTIPS providers shall comply with the FedRAMP TIC 2.0 Overlay requirements in addition to the basic requirements outlined in the DHS TIC Reference Architecture v2.0.

P. ISSO Support

P.1 The contractor Program Manager shall ensure that the contractor ISSO duties and responsibilities align with the Information Assurance and Cyber Security Division, Governance, Risk, and Compliance (GRC) Branch mission and security responsibilities. The TSA CISO is the authorizing official for ISSO designation.
Q. Continuous Diagnostics and Mitigation

Q.1 The Government, through a Continuous Monitoring as a Service (CMaaS) vendor, shall provide the contractor with GFE appliances and tools to support the implementation and maintenance of the Continuous Diagnostics and Mitigation (CDM) Solution. The tools shall be hosted on the DHS’ Infrastructure as a Service (IaaS) program. The Government, through the CMaaS vendor, shall provide sensor kits and agents that shall be deployed on all contractor Information Systems supporting the TSA.

Q.2 The contractor shall support the installation (including rack and configuration) of the sensor kits and agents on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards.

Q.3 The contractor shall tune their existing endpoint security products to coexist with the identified products to ensure smooth and cohesive functionalities. Credentials (Service accounts) shall be provided, by the TSA CISO or designee, for vulnerability scans and host interrogation.

Q.4 The Government, through the CMaaS vendor, shall provide the following support for operations and maintenance of the CDM solution sensor kits:
   - Patching (Controlled through a CMaaS Windows Server Update Service (WSUS))
   - Hardware troubleshooting & Risk Management (RMA)
   - Application maintenance (done from the Government/TSA Management Enclave)
   - Vulnerability scanning

Q.5 The contractor shall install TSA-provided CDM Solution patches within two (2) days of issuance, or as directed by TSA, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

Q.6 The TSA Contracting Owner is authorized to provide technical direction to the contractor for the sole purpose of implementing the CDM Solution. If the technical direction results in any cost incurred by the contractor, for which the contractor shall seek reimbursement from the Government, the contractor shall identify the following information in any cost/price proposal to the Government: name of system owner, summary of the technical direction, date of the technical direction, purpose of the technical direction, summary of actions taken by the contractor, any other information the contracting officer may require to further guide the directed change. The contractor shall receive approval from the Contracting Officer of the directed change prior to incurring costs associated with the technical direction.

R. Software Guidance

The Contracting Officer shall provide a listing of all TSA approved security software upon contract award. The approved security software listing is maintained by the Information Assurance Division (IAD).

R.1 In support of the CDM objective to protect high value assets (HVAs) and information, the Government has acquired security tools in order to conduct Indicator of Compromise (IOC) scans within the mandated time frame. The Government shall provide the tool license and/or equipment for installation of tool agents on all TSA supported assets.
R.2 The contractor shall support efforts to allow for the IOC scanning mandate. This may include installation of tool servers and/or agents within each system’s environment and on all TSA supported assets. The Government shall provide the contractor with the tool server(s) that shall not belong to the contractor’s system boundary. The tool server shall be reachable from OneNet/TSANet over the Internet. The tool server(s) shall be properly configured to reach all assets with the tool agent installed on the network. Credentials (service accounts) shall be provided for IOC scans and tool interrogation.

R.3 The contractor shall support or perform the installation of forensic software servlet agents on supported Operating Systems on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards. The contractor shall test and upgrade the servlet agents as directed by the IAD.

R.4 The Government shall provide the contractor with a forensic software server that shall not belong to the contractor’s system boundary. The contractor shall support or perform the installation of the server. The server shall be reachable from TSANet over the Internet and shall be primarily used for authentication and proxy functions. The server shall be properly configured to reach all assets with the agent installed on the network.

R.5 The contractor shall support efforts of incident response and forensic investigation. This includes authorization to connect TSA authorized equipment where the forensic software servlet agents are reachable to perform analysis.

R.6 The contractor shall install TSA-provided solution patches within two (2) days of issuance, or as directed by TSA CIO, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

S. Passwords

S.1 The contract ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation. In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.

T. Personal Identifiable Verification (PIV)

T.1 The Contractor shall use PIV as the primary means to access TSA resources to include IT applications and physical facility. TSA network domain user account password expiration function shall be disabled when using PIV Machine Based Enforcement (MBE). PINs for PIV card-enabled users shall not expire, and shall have a minimum six-digit PIN when logging into the network using a PIV card.

T.2 The Contractor shall ensure newly developed information system(s) support PIV smartcard authentication. The information system shall be capable to accept and electronically verify PIV credentials.

T.3 The Contractor shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. http://www.idmanagement.gov/approved-products-list.
T.4 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 TSA’s facilities, networks, and information systems.

U. **End-of-Life (EOL) / End-of-Service (EOS)**

U.1 The Contractor shall ensure that any hardware or software that is procured develops a full lifecycle plan based on the vendor’s established life and service expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within three (3) years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the TSA CISO in order to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

V. **Maintenance**

V.1 The Contractor shall ensure that the system, once operational, is properly maintained and monitored, to include: immediate response to critical security patches, routine maintenance windows to allow for system updates, and compliance with a defined configuration management process. All patches and system updates shall be properly tested in a development environment before being implemented in the production environment.

V.2 The contractor shall perform customer support twenty-four (24) hours, seven (7) days a week within the continental United States only.

W. **Security in the Agile Development Process**

All TSA systems shall follow the below guidance when delivering system and application solutions to the agency.

- All applications shall be reviewed prior to acceptance by the Contractor
- Contractor shall implement Threat Modeling
- Developer shall deliver a defect list
- Developer shall implement Patching and Configuration Management strategies
- Developer shall use Component Analysis
- Developer shall implement build tests
- Developer shall implement Manual Code Inspection
- Developer shall implement Security Regression Tests
- Developer shall implement Pre-Deployment/Post Deployment Automated Tests
- Developer shall implement industry standard “Every-Sprint Practices”, which at a minimum consists of:
  - Threat Modeling
  - Use of Approved Tools
  - Deprecate Unsafe Functions
• Static Analysis
  • Conduction Final Security Review
  • Certify, Release and Archive

•Developer shall implement industry standard Practices, which at a minimum consists of:
  • Create Quality Gates/Bug Bars
  • Perform Dynamic Analysis
  • Perform Fuzz Testing
  • Conduct Attach Surface Review

• Developer shall implement industry standard One-Time Practices, which at a minimum consists of:
  • Establish Security Requirements
  • Perform Security and Privacy Risk Assessments
  • Establish Design Requirements
  • Perform Attack Surface Analysis
  • Create Incident Response Plan

SECTION VI: Security of Systems Handling Personally Identifiable Information and Privacy Incident Response

Sensitive Information Required Special Contract Terms (MARCH 2015) SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.
“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

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

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)
Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

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

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

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the
(4) The Contractor’s invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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


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

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.
Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor’s system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

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

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

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

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

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

(f) **Sensitive Information Incident Reporting Requirements.**

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

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews,
(iv) Data analyses and processing.

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

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

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

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

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

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

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

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

(k) Security Training Requirements.

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

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

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

(End of Clause)

SECTION VII: Department of Homeland Security ISO Compliance

A. Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these
policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information.

Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

B. Security Review
The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer’s Representative (COR), and other government oversight organizations, access to the Contractor’s facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

C. Interconnection Security Agreements
Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

D. HSAR 3052.204-70 - Security Requirements for Unclassified Information Technology Resources (JUN 2006)
(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror’s proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor’s IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB
Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 5.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

E. HSAR 3052.204-71 - Contractor Employee Access (JUN 2006)

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

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

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

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

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

(End of clause)

E. HSAR 3052.204-71 - Alternate I (JUN 2006)
When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

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

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

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

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

1. The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

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

3. The waiver must be in the best interest of the Government.

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

Special Information Technology Contract Security Requirements

(a) Identification Badges. All Contractor employees shall be required to obtain and wear TSA identification badges when working in TSA facilities.

(b) Computer Access Agreement. All Contractor employees (users, managers, and operators of the TSA network) must sign TSA Form 1403, Computer Access Agreement. A copy of which shall be provided to the TSA contracting officer’s technical representative for retention for the duration of the contract.

(c) Personnel Security.

1. Privileged access users are individuals who have access to an information technology (IT) system with privileges of Administrator or above and have access to sensitive network infrastructure data. Privileged access users will be appropriately screened on entry into the privileged access position and the initial screening shall be refreshed every two years,

2. Individuals terminating voluntarily or involuntarily from a Contractor performing under contract at TSA must have an exit briefing, conducted by a supervisory or management-level employee of the Contractor in order to identify and explain their post-employment responsibilities to the TSA.

3. Records of exit interviews will be signed and maintained by the Contractor as part of the
individual employment record for a period of not less than two years following the termination of the individual’s employment.

(4) The Contractor shall notify the Contracting Officer’s Technical Representative and the Contracting Officer with proposed personnel changes. Written confirmation is required. This includes, but is not limited to, name changes, resignations, terminations, and reassignments to another contract.

(5) The Contractor shall notify the TSA, in writing of any requested change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other company engagements. The Contractor shall provide the following information to TSA: full name, social security number, effective date, and reason for change.

(6) The Contracting Officer must approve key personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 45 days from the date the completed forms are received (and acknowledged as complete) in the Security Programs Division.

(7) Failure of any Contractor personnel to pass a background investigation, without timely substitution that meets the contracts requirements, may be grounds for termination of the contract.

(d) Non-Disclosure Agreements.

(1) All TSA contractor employees and consultants must execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA) upon initial assignment to TSA and before being provided access to TSA “sensitive and/or mission critical information.” The original NDA will be provided to the TSA contracting officer’s technical representative for retention for the duration of the contract.

(2) The Contractor, and those operating on its behalf, shall adhere to the requirements of the nondisclosure agreement unless otherwise authorized in writing by the Contracting Officer.

(e) Performance Requirements.

(1) The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

(2) Contracting Officer’s Representative (COR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

SECTION VIII: Government Furnished Resources and Information

A. Office Space & Equipment
The Government shall provide on-site office space for selected Contractor personnel to work at the Government location.

For Contractor personnel performing work on Government premises, the Government will provide furniture, telephone service, workstations, software tools, access to servers and other network
components, and any other necessary equipment.

For Contractor personnel performing work offsite, the Government will provide workstations, software tools, access to servers and other network components, and any other necessary equipment.

**B. Government Furnished Property**

Work performance shall be performed on-site at the TSA Headquarters, Springfield Annex. The initial location of work will be the Springfield Annex, but the contractor can recommend that some services are completed at the contractor’s office location(s). It is the Government’s decision to accept the contractor’s proposal to complete any portion of this work offsite.

**C. Expiration of Contract/Data Disposition**

At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with TSA MD 1400.3, related Information Assurance Handbook and Technical Standards.

Proof of sanitation shall be delivered via electronic transmission (soft copy) to the COR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

**SECTION IX: Applicable Documents**

<table>
<thead>
<tr>
<th>Version</th>
<th>Document Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 9.1 or latest version</td>
<td>TSA Information Assurance Handbook</td>
</tr>
<tr>
<td>Version 12.01 or Latest Version</td>
<td>DHS 4300A Sensitive Systems Policy</td>
</tr>
<tr>
<td>Version 2.4 or Latest Version</td>
<td>RCCM Process Guide</td>
</tr>
<tr>
<td>Latest Version</td>
<td>DHS System Engineering Life Cycle</td>
</tr>
<tr>
<td>Latest Version</td>
<td>DHS Agile Development and Delivery For Information Technology Guidebook, MD 102-01-004-01</td>
</tr>
<tr>
<td></td>
<td>Apple iOS Human Interface Guidelines</td>
</tr>
</tbody>
</table>