SECTION C- STATEMENT OF WORK (SOW)

C.1.1 REQUIRING ORGANIZATION

U. S. Department of Homeland Security, Transportation Security Administration (TSA), Office of Intelligence & Analysis (OIA)

C.1.2 BACKGROUND

To enhance the security of air travel, the Secure Flight program assumed the responsibility for the passenger watch list matching functions, previously performed by aircraft operators. Secure Flight improves aviation security by identifying known and suspected terrorists and distinguishing them from the remainder of the traveling population. Based on this analysis, TSA can more effectively allocate screening resources to focus efforts on potential terrorist threats.

Secure Flight supports TSA's effort to implement intelligence-driven, risk-based screening procedures such as TSA Pre-Check. Secure Flight identifies high-and low-risk passengers in order to mitigate known and unknown threats to aviation security and designate them for enhanced screening, expedited screening, or prohibition from boarding a covered flight, as appropriate. The Secure Flight program enhances the security of domestic and international commercial air travel, by prescreening more than two million aircraft passengers a day.

C.1.3 SCOPE OF WORK

The contractor shall perform the full range of Functional Category Domain 1: Program Management, Engineering and Technology Support Services functions for ongoing Secure Flight operations and maintenance support within the following functional areas: *Optimization, Industry Performance and Analysis (IPA), Communications and Readiness (C&R), Business Architecture, Policy and Planning, Technical Support and Reporting (TS&R), and Performance Engineering PE)*. The contractor shall provide a full and adequate range of support services that meet the SOW requirements.

C.2 TECHNICAL REQUIREMENTS/TASKS

3.1 Optimization

3.1.1 Secure Flight Operations Center (SOC)

Secure Flight houses an operations center to conduct manual review of near matches to watch lists and for facilitating discussions between airlines and Secure Flight regarding inhibited passengers. The airline is required to receive government approval for the passenger to board their flight. In order for airlines to permit passengers who are potential matches to board their flight, the airline needs to contact the SOC and provide additional identity information to clear the passenger.

3.1.1.1 Implementation of Enhancements for Secure Flight Operations Center

The contractor shall provide SOC resources to develop content for system User Acceptance Testing (UAT) - user interface, case management, and knowledge management applications, quality assurance planning and other system and functional requirements. The contractor will also draft and upon

government approval, execute UAT scenarios, support training requirements for the SOC, assist in the reconfiguration of existing facilities and equipment based on new program populations and analyze the impact on SOC design and requirements, and support testing of all SOC systems including user interfaces based on system requirements and functionality.

3.1.1.2 Operations and Maintenance for Secure Flight Operations Center

Working in both classified and unclassified environments, the contractor shall provide assistance with process assessment/improvement, reporting refinement, workforce modeling, strategy, quality assessment, vetting logic/analysis, interoperability and interaction with non-Secure Flight operations, and knowledge management maintenance.

NOTE: Work within the entire Optimization area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.2 Industry Performance and Analysis (IPA)

IPA is a joint contractor and Government team responsible for onboarding airlines to Secure Flight, improving technical compliance in accordance with the Consolidated Users Guide (CUG), providing assistance in bringing new populations to Secure Flight (e.g. 12.5 carriers), and ensuring active carrier compliance with new requirements (e.g. Risk Based Security). In order to achieve these goals, a phased deployment approach has been developed and successfully implemented. The approach includes Aircraft Operator Interface Testing, Assessment, On Boarding and Production Cutover.

- Aircraft Operator Interface Testing consists of the execution of test cases to validate aircraft operator system functions and interfaces. During this phase of deployment, Secure Flight and the aircraft operators will conduct connectivity testing and system to system testing.
- After all aircraft operator interface testing is complete TSA will evaluate the test results to determine the capabilities of the aircraft operator to prepare for the next phase of deployment.
- Dn-boarding begins after the aircraft operator assessment is complete. The aircraft operator submits production passenger data to Secure Flight but the aircraft operator does not apply the boarding pass printing results at this time. Qualitative watch list matching analysis occurs during this phase and is a comparison analysis of current airline system matching results with the Secure Flight matching system. Qualitative watch list matching analysis provides the program with current aircraft operator matching results to engineer the Secure Flight system to minimize the false positive rate.
- The last phase of deployment is production cutover where the aircraft operator submits production passenger data, the Secure Flight watch list matching system processes the data and sends a boarding pass printing instruction to the aircraft operator. The aircraft operator must begin using the boarding pass printing instruction.
- After the airline has cutover to using the Secure Flight system, the contractor (with oversight from Government team members) will continually review data analysis (See Dperational Performance) with the airlines to improve system performance. They will evaluate airline data submission performance for compliance with the Secure Flight rule and system requirements.

3.2.1 Continue Airline Deployments

The contractor will support the IPA team by providing operational and technical guidance in airline

operations, system testing and system implementation strategy. This will include drafting test strategies, test plans, airline system implementation procedures and reference material for airline guidance, and maintaining the Airline Operator Data Base (AODB). To be successful, the contractor will require individuals to be subject matter experts in airline operations and system testing. The contractor will assist the IPA team in coordinating connectivity, system testing and the cutover of aircraft operator watch list matching to the Secure Flight program.

3.2.2 Operations and Maintenance for IPA

The contractor will support IPA in analyzing carrier data submissions to determine root causes, develop performance improvement plans, and assist air carriers and their respective service providers to make improvements so that their Secure Flight data submissions are made in full compliance with the Consolidated User Guide (CUG). Additionally, the contractor will provide technical expertise and guidance to the Secure Flight team to ensure Secure Flight technical systems are functioning properly with the aircraft operators.

Additionally, the contractor will provide support to the Compliance Monitoring group within IPA to assist in the evaluation of carrier behavior, develop compliance packages for use by the Office of Security Operations (OSO) and Office of Global Strategies (OGS), and form recommendations for carrier performance improvement.

3.2.3 Performance Data

IPA is responsible for collecting Secure Flight system, SOC systems, and program performance data, analyzing that data and reporting to program leadership and government stakeholders on the Secure Flight program and system performance. The program has identified over 100 performance measures that will identify system and user performance. Users include but are not limited to the airlines, SOC staff and other government stakeholders to be defined. Examples of performance measures identified so far include:

- Secure Flight System - Number of Transmissions Received, False Positive Rate, Submission Volumes by Airline, System Response Time to Airline, and System Outage.
- SOC - Manual Reviews, Selectee and No Fly Notification reports, Average Hold Time, Average Handle Time, Call Type, and Calls Handled.

3.3 Communications and Readiness

The contractor shall provide support in the areas of change management, specifically drafting communications, technical writing, document management, and training. Specific examples of work, which will be performed by the contractor, may include but not limited to:

3.3.1 Communications

- Maintain the Secure Flight Change Management (CM) Plan and associated work to include assessing current situation; develop/maintain change management strategy. The CM Plan should include CM goals and high-level activities to be supported.
- Update and maintain existing Stakeholder Assessment document.

- Maintain a comprehensive Communications and Stakeholder Outreach Plan to include, but not limited to, audience, delivery techniques to include new and existing technologies, i.e. (classroom, videoconference, webinar, etc.,), timing, frequency, key messages, communications methodology, approval processes, stakeholder satisfaction, strategy, scorecard, and feedback mechanisms.
- Maintain a list of current and approved frequently asked questions and answers.
- Develop, coordinate, and disseminate informational material for various internal and external stakeholders of Secure Flight including but not limited to Government Accounting Office, Office of Inspector General, and other agencies/departments.
- Draft informational content for press releases, public affairs guidance, and website posting and routinely review the information for irrelevant or outdated content.
- Draft and upon government approval, issue informational material on the Secure Flight Program to internal and external stakeholders (aircraft operators, travel agencies, trade associations, congress, GAO, the press etc.). Informational material will be in various forms including, but not limited to meeting content, newsletters, presentations, toolkits, job aids, correspondence, and letters.
- Support Secure Flight Program senior leadership by drafting presentations, talking points, and briefings materials.
- Provide critical analysis of information to assist in the development of accurate Secure Flight Program communications products
- Assist in building strong partnerships within Secure Flight and OIA to increase effectiveness and awareness of communications products and requirements.
- Draft and upon government approval, update and distribute Communications Standard Operating Procedures (SOP).
- Provide support to coordinate, manage and execute all aspects of aviation industry conferences.
- Draft, coordinate and disseminate periodic Secure Flight Program Newsletters.
- Support Secure Flight Program visits, tours, and demonstrations.
- Review and provide Secure Flight comment and coordination on externally produced documents.
- Archive communication products on TSA's IShare site for easy identification and retrieval.
- Assist in drafting and coordination of responses to requests for information from Congress and TSA or DHS leadership.
- Assist OIA and other offices with communications support and review of products pertaining to the Secure Flight Program.
- Additional Stakeholder Communications as required.

3.3.2 Technical Writing and Document Management

- Provide quality assurance of program communication products which are produced under section 3.5 in this SOW.
- Maintain and update the Secure Flight Style Guide, the Secure Flight glossary, and the Secure
- Flight Acronym List.

- Support key document and vital records library semi-annual reviews and updates.

3.3.3 Training

- Conduct training needs assessments for various Secure Flight entities.
- Draft training plan and training materials for Vetting Operations Division as outcome from the training needs assessments.
- Draft, maintain and refine New Hire Training course materials, transitioning appropriate modules to blended learning approach including a computer-based training.
- Deliver instructor-led courses.
    - Draft and deliver system course materials for all Secure Flight System Releases and new operational technologies based on release schedule.
    - Assist in analysis of new program initiatives to determine training requirements.
    - Propose training delivery methods and program initiated course materials to support the rollout of new features, population and capabilities based on pilot and go-live dates.
- Propose, coordinate, and facilitate Domain and Initiative Awareness programs (In-the-Know) for Vetting Operations Division.
- Draft appropriate job aids to support external stakeholders.
- Support resource management and efficiency efforts by identifying and instituting standardized training processes and tools.
- Workforce Development/Employee Development:
    - Support personnel career development by identifying appropriate training and professional development opportunities in the areas of: training opportunity awareness, curriculum development, and supervisor support.
    - Draft an employee development plan for Vetting Operations Division.
    - Draft career-progression roadmaps for non-intelligence analysts.
    - Draft a job rotation and Vetting Operations Division-level, cross-training program.
    - Support Skills Gap Analysis for employees or team to identify competency (knowledge, skills, and abilities) gaps.
    - Draft a training catalog that can be posted on IShare and maintained, available for staff to develop one-stop-shop to address performance gaps.
- Draft a database-training plan (e.g. Terrorist Identities Datamart Environment -TIDE, etc.) coordinated with other agencies and vendors.
- Draft communications on training offered by DHS/TSA/OIA and others.
- Draft performance-based process training guidance – repository of training opportunities based on performance feedback.
- Draft a "cohort" training approach that would bring supervisors from different branches together in collaborative sessions.
- Draft supervisor toolkits.

NOTE: Work within the Training area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.4 Business Architecture, Process, and Planning

The Business Architecture, Process and Planning (BAPP) functional area currently supports multiple disciplines such as: updating and maintaining current Secure Flight business process model flows and updating and maintaining current requirements in business requirements matrices and other requirement artifacts. BAPP is responsible for ensuring that all requirements are traced to system uses cases and must work closely with the Technology Solutions Division to ensure all requirements are properly implemented. The contractor will perform the following work:

3.4.1 Business Exploration

- Propose and/or draft new business processes that could streamline or support the Secure Flight business model.
- Assist in the translation of Secure Flight high-level strategic goals into business requirements.
- Support the coordination of business requirements and use cases with impacted stakeholders. Ensure deployed systems meet business requirements. Ensure User Acceptance Testing (UAT) and Validation adequately address business goals, objectives, and requirements.
- Draft concept definition papers and business cases as necessary.
- Support Secure Flight business analysts to identify and improve common business practices and ensure standardization across the Secure Flight Program and the Vetting Operations Division.
- Manage the updates and change processes related to the Secure Flight Concept of Operations (ConOps) document in alignment with the Department of Homeland Security's Strategic Plan, establish Secure Flight Program external governance plans, related processes and documentation.
- Support business continuity planning to assist the Secure Flight program; including subject matter expertise in planning and designing business continuity planning for all of the business areas of the Secure Flight program.

3.4.2 Release Planning

- Support the capture, sponsorship, and prioritization of requirements and changes for future release iterations through management of the New Idea Capture process and the Business Change Board.
- Assist to ensure proper impact assessment for change requests.
- Maintain the Program roadmap and capability prioritization pipeline.
- Support with the Technology Solutions Division to determine Secure Flight release milestones.
- Support the development and management of each release plan.

3.4.3 Requirements Management

- Draft and, upon government approval, manage business-centric requirements deliverables within each release, including documentation and validation of requirements tracing.
- Draft Business Requirement Matrices, Problem Reports (PRs) for requirements, and other requirements management artifacts, as needed (e.g. Business Architecture Document and Business Requirement Documents).
- Support business validation for tracing:

- Business requirements to Standard Operating Procedures (SOPs)
- Business requirements to system use cases.
- System use cases to test plans.
- Test plans to test results.

- Support and coordinate User Acceptance Testing (UAT) across the program.
- Log requirements and related artifacts into Secure Flight repository tools.
- Support implementation of business and operational requirements development and management processes.
- Establish mechanisms for business transition planning and management capability to ensure clear communication within the Secure Flight Program and with stakeholders. Coordinate efforts with organizational change management and ensure a smooth transition from the current state to the desired state.

3.4.4 Operational Partners Management

Support the management of relationship and coordination activities with Secure Flight operational partners, including:

- TSA Transportation Security Redress Branch (TSRB);
- TSA Office of Risk Based Security (ORBS);
- Customs and Boarder Projection (CBP); and
- Department of Justice's (DOJ's) Terrorist Screening Center (TSC).
- Assist with the documentation of operational partner agreements including Memoranda of Understanding (MOUs), Inter- and Intra- Agency Agreements (IAAs), Inter- and Intra-Departmental Agreements (IDAs), Interface Control Documents (ICDs), Service Level Agreements (SLAs), and others as needed.

3.4.5 Secure Flight Reporting

The contractor shall assist with managing the Secure Flight Reporting mailbox, including:

- Analyzing reporting data requests and confirming requirements with stakeholders.
- Researching data to satisfy requests, using available analytic tools.
- Coordinating with other teams such as Technology Support and Reporting to fulfill requests.
- Performing quality assurance on outgoing Secure Flight Reporting data and content.
- Performing ongoing stakeholder management in areas such as data quality and interpretation.
- Developing and maintaining Secure Flight Reporting SOPs.
- Collaborating with other BAPP team members to recommend and implement Business Change Requests (BCRs) resulting from Secure Flight Reporting work.
- Recommending and implementing operational process improvements, as needed.

NOTE: Work within the entire Business Architecture, Process, and Planning area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.5 Technical Support and Reporting

The contractor will support the Technical Support and Reporting team by providing resources with the technical expertise necessary to provide support for the various Secure Flight subsystems. Knowledge of the specific Secure Flight subsystems will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Data management
- Report development using Oracle Business Intelligence Enterprise Edition (OBIEE)
- Data analysis
- Root-cause analysis

3.6 Performance Engineering

The contractor will support the Performance Engineering team by providing resources with the technical expertise necessary to perform sophisticated data analysis and modeling. Knowledge of specific Secure Flight data will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Statistical data analysis
- Data extraction and manipulation (requires extensive SQL and some programming knowledge)
- Ability to convey complex information to non-technical decision makers (data visualization)
- Mathematical modeling for impact and predictive analysis
- Ability to devise processes to evaluate a closed source system

4. Project Management & Reporting and Requirements

The contractor shall perform project management services and resources required for performance under this SOW. The contractor shall comply with existing OIA and/or program- specific Configuration Management processes and procedures for hardware, software, and documentation. Specific requirements include but are not limited to:

- Contractor Work Breakdown Structure (CWBS)
- Cost, Schedule, Forecast and Performance Reporting
- Ad Hoc Reports

The contractor shall provide project management data within the monthly report, as identified in section 4.2 below.

4.1 Work Breakdown Structure

The contractor shall provide a resource-loaded contractor work breakdown structure (CWBS), outlining the proposed activities, resources and costs to complete the requirements of this SOW. This CWBS shall align seamlessly into, and reflect the respective work outlined in the Government- provided Integrated Master Schedule (IMS).

The draft resource-loaded CWBS shall be provided to the Government for approval within 10 working

days of the start of this Task Order Period of Performance. The CWBS will list the work activities, duration of each task/activity, resources required, deliverables, and cost for each work activity to be performed. This shall be the baseline CWBS, against which progress will be measured. The CO and Task Order COR. must approve any deviation from this baseline. The contractor shall report based upon a resource-loaded CWBS for schedule and requirements tracking that is proposed by the contractor and approved by the government.

4.2 Monthly Report

The contractor shall provide a monthly report outlining the contractor's cost, schedule and performance for the project by Task Order.

The contractor shall provide contractor performance reports that show the status of the contractor's production and performance assessment against the expected performance goals. Reports should show the following at a minimum:

- Reporting period
- Progress/Status
- Current month's activities (broken out to tasks performed for each effort/activity with resource assigned)
- Percentage of completion
- Forecast of next month's activities
- Issues encountered and any corrective actions during the reporting period
- Funding to date
- Cumulative dollar and percentage of funds expended
- Total funds remaining
- Projected spending for next month
- Total projected Task Order costs
- Funding shortfall date (if applicable)
- Hours expended per resource

A draft monthly reporting format will be presented to the government for approval within fourteen (14) calendar days of the start of the Period of Performance of this Task Order. The monthly report shall be submitted to the COR at least three (3) business days prior to the Program Management Review (PMR) meeting.

4.3 Ad Hoc Reports

An Ad Hoc report is a report requested by the Program Business Functional Manager addressing an area of concern not listed as a formal deliverable.

4.4 Travel

The contractor will be reimbursed for reasonable and actual costs for transportation, lodging, and meals and incidental expenses in accordance with Federal Travel Regulations (FTR). Travel performed for

personal convenience or daily travel to and from work at the contractor's facility or local government facility (i.e., designated work site) shall not be reimbursed. Prior to undertaking any travel other than local, the contractor shall submit a request for specific approval to the COR, listing names of individuals traveling and destinations, dates, purpose and estimated cost of the trip. The contractor will use the Travel Authorization form for all travel conducted. All requests for travel must be pre-approved by the government business functional lead and the COR, and must contain the information required on the Travel Request Form (see TSA IShare), to include an estimated amount not to exceed expenses consistent with Joint Travel Regulations and GSA per diem schedules.

4.5 PMR Meeting

The contractor shall conduct Monthly Program Management Reviews to present to the government information on project status to include: Performance measurements, progress towards completion, associated risks, issues and cost. The information shall be provided with summary and appropriate details of status and projected performance in the following areas: Functional performance and progress, project risks and mitigation progress, establish logical and realistic corrective action plan(s) to address identified issues, and establish priorities for execution based on the criticality of identified issue(s). Any issues identified during this review that need resolution shall be recorded and tracked by the contractor in an Action Item database. The status and disposition of all open action items shall be presented at the program review meeting, noting that disposition of each action item requires approval of the appropriate government representative - Project Manager (PM), Task Order COR, or CO. The contractor shall minimize resources and costs in connection with the monthly PMR meetings. The contractor shall conduct meetings before the fifteenth (15^{th}) business day of the month, unless otherwise directed by the government.

5. Deliverables

The following table describes the Contract Data Requirements List (CDRLs) that are required for this SOW. The Contractor requires express written approval from the CO before executing any change to the scope, content, and/or delivery schedule of the described work products and tasks in this SOW.

Table 1: Contract Data Requirements List

CDRL #	Deliverable	Description	Frequency	Reference
001	User Acceptance Testing (UAT) Analysis	Plan User Acceptance Testing Efforts: Evaluate User Acceptance Testing Results, identify system enhancements and recommend changes to improve operating efficiencies	Based on each release (estimated Quarterly)	SOW Sections 3.1.1.1 and 3.4.3
002	Parallel Testing Guidance	Write testing guides and procedures for the parallel testing phase of implementation	Update as needed	SOW Section 3.2.1

003	Parallel Testing Analysis	Create parallel testing analysis and report	As specified by airline implementation plans	SOW Section 3.2.1
004	Cutover Strategy and Criteria Plan	Write and develop airline cutover strategy and monitor individual airline cutover schedule compliance	As needed, to align with implementation of new Airline Operators	SOW Section 3.2.1
005	Cutover Readiness Review	Summarize cutover readiness for each Airline Operator	Weekly	SOW Section 3.2.1
006	Airline Operator Test Reports	Detailed results of onboard testing for each Airline Operator	At the conclusion of each Airline Operator's onboarding	SOW Section 3.2.1
007	Operational Readiness Test Plan	Write testing guides and procedures for the operational readiness testing phase of implementation	Update as needed	SOW Section 3.2.1
008	Consolidated User Guide (CUG)	Enhance/modify the Consolidated User Guide (CUG)	Update as needed	SOW Section 3.2.1
009	Secure Flight Style Guide, Acronym List, and Glossary	Maintain the Secure Flight style manual (guide), acronym list, and glossary	Quarterly updates as needed. Final Assessment Due at end of TO	SOW Section 3.3.2
010	Secure Flight Comprehensive Training Plan	Maintain comprehensive training plan which outlines objectives, needs, strategy, timelines and curriculum for Vetting Operations Division training	Annual updates as needed. Final Assessment Due at end of TO	SOW Section 3.3.3
011	Training Materials	Create/maintain training material detailed in the Secure Flight training plan	As specified in the Secure Flight Training Plan	SOW Section 3.3.3
012	Workforce Development/ Employee Development	Create/maintain employee development initiatives as identified in the employee development plan	Quarterly Submission of artifacts created. Annual updates as needed	SOW Section 3.3.3

013	Secure Flight Business Architecture	Modifications and/or enhancements to Secure Flight business requirements and business process model/flows	Due per functionality/project implementation and release (estimated Quarterly) Ad Hoc Emergency Process Change Requests	SOW Section 3.4.3
014	Ad-hoc and recurring reports	Various reports to transmit Secure Flight data to stakeholders to inform decision-making	Create as needed	SOW Sections 3.2.3, 3.5 and 3.6
015	Contractor Work Breakdown 5tructure (CWB5)	Resource-loaded schedule, including cost, performance, and requirements tracking that the Contractor proposes and is approved by the Government for each Task Order. The CWB5 contains scheduled work products and related services for each mission application and align with the program's IMS (if provided)	10 Working Days after Task Order issued, updates as needed	SOW Section 4.1
016	Monthly Report	Cost, Schedule, and Performance Report	Draft: Within 14 calendar days of the start of the Period of Performance of each Task Order Monthly: no later than 10th Business day of	SOW Section 4.2
017	Program Management Reviews (PMRs)	Monthly meeting to discuss 5chedule, Costs, Resources, Technical issues, problems and resolutions	No later than the 15th Business Day of each month	5OW Section 4.5
018	Final Report	Summarizes support activities, "start to completion schedules", deliverables and results achieved relative to the performance objectives of this SOW	Draft report 15 working days prior to conclusion of work. Final report 5 working days after receipt of comments	SOW 5ection 5

019	Firm Fixed Price Proposal & SOW	Detailed Scope of Work with tasks breakdown and deliverables identified	No later than 90 days before execution of exercising the Option Period	SOW Section B.2

The dates shown in the Deliverables Table are the required initial delivery date, which initiates the government acceptance timeline described below. All plans and documents are intended to provide continuity with previous work performed and to provide a comprehensive set of program management guidance and reporting as well as systems development and management documentation.

All deliverables, existing plans and documents shall be used in their current form where applicable and shall be updated as appropriate to accommodate deficiencies, program and development changes. Documents listed but not currently existing shall be created and delivered at the time specified in the frequency column above. The contractor shall prepare and maintain all documentation in accordance with an industry standard best practice for auditable, repeatable engineering process to assure the availability and accuracy of a comprehensive, complete, and current set of plans, reports, and documents.

The contractor shall use the TSA Systems Development Life Cycle Guidance Document, version 2.0, (or updated version) for updating of systems development documentation form and content.
The list of documents and their content and format may be refined and tailored by mutual agreement between the government and contractor to assure quality program management, systems development, and systems operation and management. The contractor shall also use the TSA Style Guide when preparing all deliverables. The Style Guide can be found on the TSA intranet at:

http://tsaweb.tsa.dot.gov/tsaweb/intraweb/assetlibrary/web_best_practices_and_style_guide.pdf

(END OF SECTION C)

SECTION D - PACKAGING AND MARKING

D.1 Markings

All deliverables submitted to the TO Contracting Officer or the TO Contracting Officer Representative (COR) shall be accompanied by a packing list or other suitable shipping documentation that shall clearly indicate the following:
(a) Contract number;
(b) Task order number;
(c) Name and address of the consignor;
(d) Name and address of the consignee;
(e) Government bill of lading number covering the shipment (if any); and
(f) Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).

(END OF SECTION D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

All contract deliverables, including documents and system implementations, require approval and formal acceptance by the Task Order COR. The Government will have up to 10 business days after receipt of a deliverable to accept or reject any deliverable. If the Task Order COR rejects a deliverable, the Contractor will be provided specific written comments detailing the basis for the rejection and recommended corrective action. The Contractor shall have up to 10 calendar days to address all specific written comments by either incorporating the requested Government changes or providing an explanation of why the Government-requested changes are not being incorporated. The Government will have an additional five (5) calendar days to review and provide a final decision regarding acceptance or rejection of the deliverable.

E.2 Scope of Inspection

Documents submitted by the Contractor shall be professional in content and presentation according to commonly accepted standards of writing and editing in the subject field. The Contractor shall provide electronic copies to the Government Program Manager, Task Order COR, Contracting Officer and any other specified Government representatives as directed by the Government when due. All documents shall be delivered in Microsoft Office format (including Word, Excel, PowerPoint, Access, Visio, and Project) or other formats accepted by the government by direction of the Task Order COR. Previously released documentation will be delivered in current format unless mutually agreed otherwise.

E.3 Basis of Acceptance

Final CDRL deliveries shall be accompanied with a letter of delivery and Government acceptance to be signed by the Task Order COR and Project Manager (PM).

E.4 Review of Deliverables

At any point in the process of the review of deliverables, the deliverable is considered accepted if the Government provides written acceptance or does not provide comments and/or change requests within fifteen (15) business days of the receipt of the deliverable.

E.5 Final Deliverables

The contractor shall provide two (2) Compact Disk- Read Only Memory (CD-ROM) copies of the set of all final documents at the end of each Task Order. All documents shall be delivered in a format mutually agreed to between the contractor and the government. Previously released documentation will be delivered in current format unless mutually agreed otherwise. CDRL content may be combined into one delivered document with notification.

(End of Section E)

SECTION F- PERFORMANCE

F.1 PERIOD OF PERFORMANCE

The period of performance for this task order will be for a base period of twelve (12) months from award date with two (2) 12 month option periods and one (1) seven month option period to end June 21, 2018. The period of performance will start upon all contractor personnel's completion of TSA's personnel security process and deemed suitable/eligible to start work.

F.2 PLACE OF PERFORMANCE

Contractor's personnel will work full-time during core hours (0800-1800) at TSA Annapolis Junction location. Frequent visits to TSA Headquarters location may be necessary in some circumstances and will be coordinated and approved by the COR and the contractor Program Manager. The contractor is expected to provide on-site support during this timeframe on an 8-hour per day, 5-day a week basis.

U.S. Department of Homeland Security
Transportation Security Administration
132 National Business Parkway
Annapolis Junction, MD 20701

F.3 GOVERNMENT FURNISHED FACILITIES

The Government identifies the following GFE and GFI for this effort:

- Use of Government-provided facilities for contractor office space;
- Computer-hosting facilities with appropriate power, space and environment;
- Operating environments to include a workstation;
- Documentation required for facility and system accreditation;
- OIA On/Off-boarding procedures and;
- Access to TSA's Online Learning Center (OLC) – TSA's automated training system used to meet the mandated privacy and security training requirements.
- Necessary access to the TSA Intranet (internal website) and related software tools
- Access to copier and duplicating equipment

F.4 TRAVEL REQUIREMENTS

Long distance Travel is required in support of this Task Order. The Government will reimburse travel in accordance with the Federal Travel Regulations. All travel must be pre-approved by the COR.
Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed.

(END OF SECTION F)

SECTION G- CONTRACT ADMINISTRATION DATA

G.1. CONTRACTING OFFICER (CO)

The Contracting Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue orders, obligate funds and authorize the expenditure of funds, and notwithstanding any term contained elsewhere in this contract, such authority remains vested solely in the Contracting Officer. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) In the event, the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:
NAME: Joseph Wolfinger
PHONE NUMBER: 571-227-3118
EMAIL: Joseph.Wolfinger@tsa.dhs.gov

G.2. CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COR) AND TECHNICAL MONITORS

1. The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

2. The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

TSA CDR:
NAME: Anthony Pinto
PHONE NUMBER: 240-568-5307
EMAIL: Anthony.Pinto@tsa.dhs.gov

3. The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

4. The responsibilities and limitations of the COR are as follows:
   - The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
   - The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
   - The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
   - The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
   - The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
   - The COR is not authorized to direct the Contractor on how to perform the work.
   - The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
   - The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

5. The responsibilities and limitations of the TM are as follows:
   - Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.
   - Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
   - Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
   - Informing the COR if the Contractor is not meeting performance, cost, and schedule milestones.
   - Performing technical reviews of the Contractor's proposals as directed by the COR.
   - Performing acceptance of the Contractor's deliverables as directed by the COR.
   - Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

G.3 SUBMISSION OF INVOICES

(a) Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

(b) Invoice Submission Method: Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:
1) Facsimile number is: 757-413-7314

The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (e) of this clause.

2) U.S. Mail:
United States Coast Guard Finance Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake, VA 23327-4111

3) Email Invoices:
FIN-SMB-TSAInvoices@uscg.mil or
www.fincen.uscg.mil

(c) Invoice Process: Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Technical Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

(d) Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

(1) Via the internet: https://www.fincen.uscg.mil
Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

(2) Via the Payment Inquiry Form: https://www.fincen.uscg.mil/secure/payment.htm

(e) Invoice Elements: Invoices will automatically be rejected if the information required in subparagraph (a) (2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and DUNS number are not included in the invoice. All invoices must be clearly correlate invoiced amounts to the corresponding contract line item number and funding citation.

(f) Supplemental Invoice Documentation: Contractors shall submit all supplemental invoice documentation (e.g. copies of certified time sheets (as applicable), subcontractor invoices, receipts, signed receiving reports, travel vouchers, etc) necessary to approve an invoice along with the original

invoice. The Contractor invoice shall contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Invoice charges shall be billed per appropriate Contract Line item Number (CLIN), period of performance and obligated funding. Unless otherwise authorized by fiscal law, funding from one CLIN may not be utilized to offset charges on another CLIN, specifically if it is different accounting and appropriation data. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Technical Representative.

(h) Frequency of Invoice Submission: Invoices may be submitted on a bi-weekly or monthly basis. Once the invoicing method has been chosen, this method shall be the frequency of invoicing for the life of the Task Order.

(END OF SECTION G)

SECTION H- SPECIAL REQUIREMENTS

H.1 DISCLOSURE OF INFORMATION

Information furnished by the Contractor under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personally-identifiable information must be clearly marked.
Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the requirements of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.
In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and information and must ensure that all work performed by its Subcontractor(s) shall be under the supervision of the Contractor or the Contractor's employees.

H.2 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION

Publicity releases in connection with this contract shall not be made by the Contractor unless prior written approval has been received from the Contracting Officer.
The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.
A minimum of five full business days' notice is required for requests made in accordance with this provision.

H.3 CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES

If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

H.4 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.
(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.5 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

The T5A may enter into contractual agreements with other Contractors (i.e., —Associate Contractors) in order to fulfill requirements separate from the work to be performed under this contract, yet having a relationship to performance under this contract. It is expected that contractors working under TSA contracts will have to work together under certain conditions in order to achieve a common solution for T5A. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant Contracting Officer (CO) and/or designated representative in providing suitable, non-conflicting technical and/or management interface and in avoidance of duplication of effort. Information on

deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.
Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant CO and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.
Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a —lead Contractor for the project. In these cases the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.
Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

H.6 NON-PERSONAL SERVICES

—Personal services are those in which contractor personnel would appear to be, in effect, Government employees via the direct supervision and oversight by Government employees. No personal services shall be performed under this contract. No Contractor employee will be directly supervised by a Government employee. All individual Contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor of the Contractor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.
The Contractor shall not perform any inherently governmental actions as defined by FAR 7.500. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change any contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.
The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this clause. Nothing in this special contract requirement shall limit the Government's rights in any way under any other term of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this special contract requirement shall be included in all subcontracts at any tier.

H.7 CONTRACTOR RESPONSIBILITIES

The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.
The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government

and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.
A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition.
The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall not:
Discuss with unauthorized persons any information obtained in the performance of work under this contract. Conduct business not directly related to this contract on Government premises.
Use computer systems and/or other Government facilities for company or personal business other than work related; or
Recruit on Government premises or otherwise act to disrupt official Government business.

H.8 QUALIFICATIONS OF EMPLOYEES

The Contracting Officer may require dismissal from work under this contract and/or removal of access to government facilities, property, information and/or information systems of those employees which the Contracting Officer deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment the Contracting Officer deems contrary to the public interest or inconsistent with the best interest of national security.

H.9 NON-DISCLOSURE AGREEMENTS

Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive But Unclassified, Government procurement sensitive information, and/or other sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

H.10 OBSERVANCE OF LEGAL HOLIDAYS

The Government observes the following holidays:

New Year's Day	*Martin Luther King Birthday*
President's Day	*Memorial Day*
Independence Day	*Labor Doy, Columbus Day*
Veteran's Doy	*Thanksgiving Day*
Christmas Day	*Inauguration Doy (Washington, DC metropolitan area)*

In addition to the days designated as holidays, the Government observes also the following days:
Any other day designoted by Federal Stotute,
Any other day designoted by Executive Drder, and
Any other day designoted by President's Proclamation.

Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be

reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Technical Representative.
In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursable and time and material (T&M) contracts, the government will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.
Otherwise, the management responsibility for contractor functions approved by the Contracting Officer for offsite work, in the event of inaccessibility of federal workplaces are the sole responsibility of the contractor. The contractor may propose telework or other solutions when critical work is required, however, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location and all resources necessary to complete such performance.
In the event of an actual emergency, the Contracting Officer may direct the contractor to change work hours or locations or institute tele-work, utilize personal protective equipment or other mandated items.

H.11 ADVERTISING OF AWARD

The contractor shall not refer to contract awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

H.12 MAJOR BREACH OF SAFETY OR SECURITY

(a) Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Safety is essential to TSA and compliance with safety standards and practices is a material part of this contract. A major breach of safety may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of safety must be related directly to the work on the agreement. A major breach of safety is an act or omission of the Contractor that consists of an accident, incident, or exposure resulting in a fatality, serious injury, or mission failure; or in damage to equipment or property equal to or greater than $1 million; or in any "willful" or "repeat" violation cited by the Occupational Safety and Health Administration (OSHA) or by a state agency operating under an OSHA approved plan.

(b) Security is the condition of safeguarding against espionage, sabotage, crime (including computer crime), or attack. A major breach of security may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of security may occur on or off Government

installations, but must be related directly to the work on the agreement. A major breach of security is an act or omission by the Contractor that results in compromise of classified information or sensitive security information or sensitive but unclassified information, including contractor proprietary information, illegal technology transfer, workplace violence resulting in criminal conviction, sabotage, compromise or denial of information technology services, equipment or property damage from vandalism greater than $250,000, or theft greater than $250,000.

NOTE: Breach of Security for the purposes of this definition should not be confused with breach of security in screening operations.

(c) In the event of a major breach of safety or security, the Contractor shall report the breach to the Contracting Officer. If directed by the Contracting Officer, the Contractor shall conduct its own investigation and report the results to the Government. The Contractor shall cooperate with the Government investigation, if conducted.

H.13 CONTRACTOR STAFF TRAINING

The contractor shall provide fully trained and experienced personnel. Training of contractor personnel shall be performed by the contractor at its expense, except as directed by the Government through written authorization by the Contracting Officer to meet special requirements peculiar to the contract. Training includes attendance at seminars, symposia or user group conferences. Training will not be authorized for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer languages and computer operating systems that are available on the commercial market or required by a contract. This includes training to obtain or increase proficiency in word processing, spreadsheets, presentations, and electronic mail.

H.14 EMPLOYEE TERMINATION

The contractor shall notify the Contracting Officer immediately whenever an employee performing work under this contract who has been granted access to government information, information systems, property, or government facilities access terminates employment. The contractor shall be responsible for returning, or ensuring that employees return, all DHS/TSA -issued contractor/employee identification, all other TSA or DHS property, and any security access cards to Government offices issued by a landlord of commercial space.

H.15 STANDARDS OF CONDUCT AND RESTRICTIONS

The contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. Personnel performing work under this contract shall not:
Solicit new business while performing work under the contract;
Conduct business other than that which is covered by this contract during periods paid by the Government;

Conduct business not directly related to this contract on Government premises; Use Government computer systems or networks, and/or other Government facilities for company or personal business; Recruit on Government premises or otherwise act to disrupt official Government business.

H.16 ELECTRONIC AND INFORMATION TECHNOLOGY TO ACCOMMODATE USERS WITH DISABILITIES (SECTION 508 OF THE REHABILITATION ACT)

Section 508 of the Rehabilitation Act prohibits federal agencies from procuring, developing, maintaining, or using electronic and information technology (EIT) that is inaccessible to people with disabilities. The applicable standards in Section 508 of the Rehabilitation Act, as amended, shall apply to this contract and any items, or services covered by or provided in connection with this requirement. The Contractor shall provide items and services that comply with Section 508 requirements and the Electronic and Information Accessibility Standards at 36 CFR Part 1194.

H.17 WORKPLACE VIOLENCE PREVENTION

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be required to complete Workplace Violence Prevention training available through the TSA Online Learning Center. The course, entitled "Preventing Workplace Violence at TSA" shall be completed within 60 days of onboarding.

H.18 NOTIFICATION OF PERSONNEL CHANGES

The Contractor shall notify the Contracting Officer's Technical Representative (COR) in writing of any changes needed in building, information systems, or other information access requirements for its employees in order to meet contract requirements not later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to the COR: full name, social security number, effective date, and reason for change.

H.19 SUBSTITUTION OF KEY PERSONNEL

The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract's requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

(a) an explanation of the circumstances necessitating the substitution;
(b) a complete resume of the proposed substitute; and
(c) any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

H.20 CONTROLLED UNCLASSIFIED INFORMATION DATA PRIVACY AND PROTECTION

The Contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the Government ii) Government data transmitted by the contractor, and iii) Government 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 Government data, including but not limited to Personal Identifiable Information (PII), Sensitive Security Information (SSI), and Sensitive But Unclassified (SBU), and/or Critical Infrastructure Information (CII), shall be protected according to Department of Homeland Security information security policies and mandates.
At the expiration of the contract, the contractor shall return all Government information and IT resources provided to the contractor during the contract.
The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow all applicable DHS Component Agency's requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI, Informational Security and Privacy training, if required by the DHS Component Agency
The Contractor, and those operating on its behalf, shall adhere to the requirements of the non-disclosure agreement unless authorized in writing by the Contracting Dfficer.
The Government will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment as applicable. If encryption is required, the following methods are acceptable for encrypting sensitive information:

a. Products Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

The contractor shall maintain data control according to the applicable DHS Component Agency's security level of the data. Data separation will 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 must comply with TSA MD 3700.4 if applicable.
Users of Government 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 Government IT assets are expected to actively apply the practices specified in the TSA Information Technology Security Policy (ITSP) Handbook, Chapter 3, Section 6, Privacy and Acceptable Use, or similar DHS Component Agency's guidance or policy.
The contractor shall comply with the all data disposition requirements stated in the applicable DHS Component Agency's Information Security Policy. For all TSA orders the contractor shall comply with Information Security Policy Handbook Chapter 3, Section 17 Computer Data Storage Disposition, as well as TSA Management Directive 3700.4.

H.21 PER5ONNEL ACCESS

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be subject to the security procedures set forth in this contract.

H.22 SUITABILITY DETERMINATIDN FOR CONTRACTDR EMPLDYEES

All contractor employees seeking to provide services to TSA under a TSA contract are subject to a suitability determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Office of Security, Personnel Security Division (PerSec), will allow a contractor employee to commence work on a TSA

contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

A suitability determination involves the following three phases:

Phase 1: Enter On Duty Suitability Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination will include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final suitability determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed suitable to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Technical Representative (CDTR) of the favorable determination. Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for final suitability adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

Phase 3: Final Suitability Adjudication: TSA PerSec will complete the final suitability determination after receipt, review, and adjudication of the completed OPM background investigation. The final suitability determination is an assessment made by TSA PerSec to determine whether there is reasonable expectation that the continued employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final suitability determination will result in a notification to the COTR that the contractor employee has been deemed unsuitable for continued contract employment and that he/she shall be removed from the TSA contract.

H.23 SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE

(a) Definitions.

—Breach (may be used interchangeably with —Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any

similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.
—Personally Identifiable Information (PII) as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.
Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII) as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:
Driver's license number, passport number, or truncated SSN (such as last 4 digits)
Date of birth (month, day, and year)
Citizenship or immigration status
Financial information such as account numbers or Electronic Funds Transfer Information Medical Information
System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)
Other Personally Identifiable information may be —sensitive depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.
Sensitive PII have higher impact ratings for purposes of privacy incident handling.
(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding its systems, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.
(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4
In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;
(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements
(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
(6) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
(i) Authorized and official use;
(ii) Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;
(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.
(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.
The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.
(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.
(f) Personally Identifiable Information Notification Requirement. The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.
In the event that a PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.
(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

H.24 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 all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 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 non-disclosure 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 Technical Representative (COTR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

H.25 Contract Status Review

a. Background. Prompt, accurate data gathering, analysis and reporting enables both the Contractor and the Government to make sound decisions relating to performance under the contract. While the Contractor is solely responsible for performance, the Government wishes to be informed on all actions under the contract that affect compliance with contract cost, performance or schedule compliance.

b. Reporting Content. The Contractor shall provide information according to the slides included in the Contractor In-Process Status Review template that is attached to this contract. A matrix describing each slide and its reporting requirements follows:

Slide title	Deliverables
Requirement for contractor's reporting	The contractor shall identify each major deliverable under the contract and identify the required delivery date and those activities that the contractor has identified as critical to meet that delivery date

Slide title	Schedule
Requirement for contractor's reporting	The contractor shall report each item under the contract's schedule with the planned and actual dates for deliveries identified.

Slide title	Upcoming Events
Requirement for contractor's reporting	The contractor shall identify significant upcoming events as planned under or related to the contract that relate to contract performance.

Slide title	Human Resources/Staffing
Requirement for contractor's reporting	The contractor should include the elements as listed on the slide, with particular attention devoted to the extent to which the key personnel identified under the contract (by their positions) are actually filled and performing or what exact activities are underway to hire suitable candidates for performance.

Slide title	Risks
Requirement for contractor's reporting	The contractor shall report each risk area earlier identified (a red or yellow status item, anticipated cost overrun or late deliverable) and provide an assessment of the risks to the contract performance if the item is not capable of being remedied in time to attain the required contract performance.

Slide title	If Firm-Fixed Price
Requirement for contractor's reporting	The contractor should discuss delivery schedule compliance.

c. Reporting Method. The Contractor shall convene a meeting, located at the mutual convenience of the Contractor and Government that will include the Contractor's principal managers directing contract performance in which to explain the information presented in the attached slides. All persons identified as contractor "key personnel" in the attached contract will present the information contained in or related to their particular area of the contract status reporting template. The Government's Contracting Officer, Contracting Officer's Technical Representative, the Program Manager and other relevant Government personnel will attend. The Contractor should be able both to present information called for on the slide templates as well as questions from the Government related to them. During the course of the contract, this status reporting process is expected to generate action items for the contractor to address, and the status and progress of resolving each action item must be addressed at each meeting.

d. Reporting Frequency. The Contractor shall report the template information on a quarterly basis. The contractor shall deliver a copy of the final prepared charts for the required briefing to the COTR and Contracting Officer not later than two business days prior to the scheduled meeting.

e. Additional Requirements. The Government may, at its discretion, require additional items to be reported through the course of the contract and will provide additional instructions concerning such.

f. The effort required gathering data, report such, and conduct the required reporting process is included in the total price of this contract, and no activity related to these required status reports will be available for any further adjustment under the contract.

H.26 5200.225.001 Notice to Offerors/Contractors Concerning Trade Agreements terms applicability to the Transportation Security Administration (APR 2014)

With respect to the following Federal Acquisition Regulation (FAR) provisions and clauses listed directly below:

FAR 52.225-1 "Buy American Act—Supplies,"
FAR 52.225-2 "Buy American Act-Certificate,"
FAR 52.225-5 "Trade Agreements,"
FAR 52.225-6 "Trade Agreements Certificate,"
FAR 52.225-9 "Buy American Act—Construction Materials,"
FAR 52.225-10 "Notice of Buy American Act Requirement-Construction Materials,"
FAR 52.225-11 "Buy American Act—Construction Materials under Trade Agreements," and FAR 52.225-12, "Notice of Buy American Act Requirement—Construction Materials under Trade Agreements"

Offerors are hereby notified that the World Trade Organization Government Procurement Agreement presently makes the Transportation Security Administration (TSA) subject only to sources from within the following signatory countries: Canada, Chinese Taipei, Hong Kong, Israel, Liechtenstein, Norway, European Union, Iceland, and Singapore. Otherwise, the only other trade agreements that presently cover the TSA are the North American Free Trade Agreement and the U.S.-Chile Free Trade Agreement. The TSA cannot evaluate offers or award contracts to sources from countries not covered in these identified trade agreements or as specified herein. Offerors must analyze their intended proposals and provide information in response to the required provisions accordingly.

The European Union participation is as defined at
http://www.wto.org/english/thewto_e/countries_e/european_communities_e.htm

H.27 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.
(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.28 TECHNICAL INSTRUCTION

(a) Performance of the work described herein may be subject to written or oral technical instructions issued by the Contracting Officer's Representative specified in Section 11.2 of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "Changes" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.
(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.
(d) Failure of the Contractor and the CO to agree on whether Government direction is technical direction or a Change within the purview of the "Changes" clause shall be a dispute concerning a question of fact within the meaning of the Clause of the General Provision entitled, "Disputes."
(e) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

H.29 5200.231.001 TRAVEL AND PER DIEM (APPLICABLE TO COST REIMBURSEMENT AND T&M TYPE CONTRACTS ONLY) (AUG 2013)

The Contractor shall be reimbursed for travel costs associated with this contract. The reimbursement for those costs shall be as follows:

- Travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.
- Per diem will be reimbursed, at actual costs, not to exceed, the per diem rates set forth in the Federal Travel Regulations prescribed by General Services Administration and when applicable, Standardized Regulations Section 925 – Maximum Travel Per Diem Allowances for Foreign Areas – prescribed by the Department of State.
- Travel of more than 10 hours, but less than 24 hours, when no lodging is required, per diem shall be one-half of the Meals and Incidental Expenses (M&IE) rate applicable to the locations of temporary duty assignment. If more than one temporary duty point is involved, the allowance of one-half of the M&IE rate is prescribed for the location where the majority of the time is spent performing official business. The per diem allowance shall not be allowed when the period of official travel is 10 hours or less during the same calendar day.
- Airfare costs in excess of the lowest rate available, offered during normal business hours are not reimbursable.
- All reimbursable Contractor travel shall be authorized through the issuance of a task order executed by the Contracting Officer.

Local Travel Costs will not be reimbursed under the following circumstances:

- Travel at Government installations where Government transportation is available
- Travel performed for personal convenience/errands, including commuting to and from work; and

- Travel costs incurred in the replacement of personnel when such replacement is accomplished for the Contractor's or employee's convenience.

H. 30 5201.242.001 PERIOD OF PERFORMANCE FOR CONTRACTS REQUIRING EMPLOYEE BACKGROUND CHECKS (AUG 2013)

The period of performance begins 60 days after contract award to allow for the Enter On Duty Suitability Determination. A contract modification shall be executed to revise the period of performance if the determination process is completed earlier.

(END OF SECTION H)

SECTION I- ADDITIONAL CLAUSES

The terms and conditions of the DHS TABSS Schedule shall govern with the following FAR and HSAR clauses that are either incorporated by reference or provided in full text herein. The complete text can be found at http://farsite.hill.af.mil/farsite_alt.html and click on current FAR and HSAR then select the appropriate clause.

I.1 52.204-1 APPROVAL OF CONTRACT (DEC 1989)

This contract is subject to the written approval of the Contracting Officer and shall not be binding until so approved.
(End of clause)

I.2 52.204-2 SECURITY REQUIREMENTS (AUG 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."
(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

I.3 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in section 31.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Department of Homeland Security
Transportation Security Administration
Office of Acquisition TSA-25
Attn: Joseph Wolfinger
601 South 12th Street Arlington, VA 20598-6025

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(END OF SECTION I)

SECTION J- ATTACHMENTS

J-1	Non- Disclosure Agreement (to be executed on date of award)
J-2	Labor Category Table
J-3	SSI Cover Sheet
J-4	DD 254

(END OF SECTION J)

SECTION L- INSTRUCTIONS, CONDITIONS AND NOTICES

1.0 PAYMENT OF PROPOSAL COSTS

This solicitation does not commit the Government to pay any cost incurred in the submission of the proposal or in making necessary studies or designs for the preparation thereof, nor to contract for services or supplies.

2.0 52.216-1 TYPE OF CONTRACT (APR 1984)

The Government contemplates award of a single Task Order that will be Time &Materials and shall include a CLIN for Other Direct Costs (Travel) (i.e. non-labor requirements). This Task Order may be converted to FFP at exercise of Option period.

3.0 ADDENDUM TO 52.212-1 - INSTRUCTIONS TO OFFERORS COMMERCIAL ITEMS

A. Proposals shall consist of an Oral Presentation and a Written Response. The Written Response shall consist of a Cover Letter, Copy of Slides to be used by the Offeror in support of the Oral Presentation, Commitment Letters for identified Key Personnel, response to Factor 3 "Past Performance" and Factor 4 "Price/Cost".

Each Offeror is allowed a maximum total of 90 minutes for the Factor 1 and Factor 2 Oral Presentations; the 90 minutes may be allocated between Factor 1 and Factor 2 as the contractor discretion.

In order to be eligible for award, Offerors must provide a Proposal consisting of the following:

PROPOSAL	FACTOR	PAGE LIMIT	SOLICITATION ATTACHMENT TO BE COMPLETED BY OFFEROR
ORAL	FACTOR 1 - Management & Technical Approach	**Oral Presentation – No Page Limit, but only slides submitted with proposal and used during the Oral Presentation will be evaluated.**	N/A
	FACTOR 2- Key Personnel & Staffing approach	**Oral Presentation--Copy of Slides to be used by the Offeror in support of the Oral Presentation. No Page Limit, but only slides submitted with proposal and used during the Oral Presentation will be evaluated**	N/A
WRITTEN	Cover Letter	One (1) Page	N/A

VOLUME I	FACTOR 1 – Management & Technical Approach	Copy of Slides to be used by the Offeror in support of the Oral Presentation.	N/A
	FACTOR 2 – Key Personnel & Staffing Approach	**Copy of Slides to be used by the Offeror in support of the Oral Presentation.** **Commitment Letter(s) – No Page Limit.** **Key Personnel Resumes- No Page limit.** **Staffing approach spread sheet- No page limit**	N/A
VOLUME II	**Cover Letter**	**One (1) Page**	**N/A**
	FACTOR 3 – Past Performance	No more than 3 references- No page limit	N/A
VOLUME III	**Cover Letter**	**One (1) Page**	**N/A**
	FACTOR 4 – Price/Cost	**Completed SECTION B table - No Page Limit** **Completed Staffing Plan table - no page limit**	**Pages 2-8** **Page 53**

B. Proposals must be clear, coherent, and prepared in sufficient detail for effective evaluation. Proposals must include convincing rationale and substantiation of all claims. Offerors shall assume that the Government has no prior knowledge of their experience and will base its evaluation on the information presented in the Offeror's Proposal.

C. Proposals shall be clearly marked with the solicitation number, "HSTS04-14-R-OIA072" and include a Cover Letter.

D. Minimum Proposal Acceptance Period. The Government requires a minimum acceptance period of at least 180 calendar days from the Proposal due date. A proposal allowing less than the Government's minimum acceptance period may be rejected.

E. In the event an Offeror is concerned that information submitted in response to this Solicitation contains confidential financial and proprietary information, including trade secrets, then such information must be clearly marked. In the event an Offeror considers specific information to be confidential they shall provide a written declaration containing supporting rationale for their contention that the information constitutes an exception to release under Federal law.

F. Any information that has been clearly marked as confidential financial and proprietary will be considered as potentially constituting an exception to release. In such cases, the Government will attempt to release the information after redacting the specific information identified as confidential financial and proprietary and notify you.

G. Offerors are encouraged to use graphic presentations where such presentations will contribute to the compactness and clarity of the Proposal.

H. **All written response information submitted in response to this solicitation, inclusive of graphics, shall be formatted on 8 ½" x 11" size paper, use 12-point sized font, single line spacing, and 1-inch margins. Tables, figures and graphs may use 9 point font. All pages must be numbered.**

4. PROPOSAL SUBMISSION REQUIREMENTS

A. ORAL PRESENTATION

Offerors who submit the required written response, defined in Section L.3., will be invited to provide an in-person oral presentation addressing the proposed Management and Technical approach and Key Personnel and Staffing approach as outlined below. The offerors must present only what is in their written proposal. If TSA finds that the slides during the presentation differ from what was submitted electronically, the electronic copy received in response to the solicitation shall govern. No price information shall be included in the presentation narrative or briefing slides.

Scheduling of oral presentations will be done through random selection. TSA reserves the right to reschedule oral presentations at the sole discretion of the Contracting Officer if necessary. Submission of video tapes or other forms of media containing the presentation for evaluation, in lieu of the in-person oral presentation, will be rejected.

Date/Time: When scheduling the presentations, TSA will advise Offerors of the date and time of its presentation on July 24, 2014. Presentations are tentatively scheduled to occur from July 28, 2014 through August S, 2014 and is subject to change.

Location: Oral presentations will be held at TSA headquarters in Arlington, VA.

Attendees: The number of Offeror attendees is limited to six (6) people. Offerors shall have the option of selecting the participants to make the presentation; however, Offerors are encouraged to select from the individuals proposed to fill key roles.

Time Limit: Oral presentations are limited to Ninety Minutes in duration, exclusive of any Question and Answer period. Any set-up of visual aids and remarks made by the Contracting Officer prior to the presentation will not count against the Offeror's 90 Minute time limit. The Government will not be

allowed to evaluate any of the information in the slide deck (See Documentation below) that is not presented during the Offeror's 90 Minute time limit.

Question and Answer (Q&A) Period: The Government anticipates a Q&A period with the Offeror after the completion of the oral presentation. If a Q&A period is necessary, after completion of the oral presentation, the Government will excuse the Offeror from the presentation room to formulate relevant clarification questions and topics pertaining to the presented material. The Offeror will then be notified by the Contracting Officer that they may return back to the presentation room wherein the clarification questions and or discussion topics will be communicated by the Contractor Officer to the Offeror. The Offeror will then be permitted to excuse itself, for a maximum of 30 minutes, to allow for a proper response. The response by the Offeror will constitute as a component of the oral presentation, and the Offeror's response is limited to 30 minutes. The time required for the Q&A period with Offerors will not be counted against the Offeror's 90 Minute time limit.

Documentation: The TSA will not be audio or video recording the presentation. All Offerors shall document the oral presentations on briefing slides and provide five (5) printed copies of the slides at the time of the oral presentation. The Government will only evaluate the slides presented as part of the oral presentation. For example, if the Offeror provides a ten (10) page presentation at the time of the oral presentation, but only addresses the first nine (9) slides as part of the presentation, the Government will only evaluate slides one (1) through nine (9), and will not evaluate slide number ten (10). These briefing slides will be used as a record of oral presentations to document what the Government relied upon in making the source selection decision in accordance with FAR 15.102(e). The Government will not accept for evaluation any additional documentation (such as procedures, manuals, administrative handbooks or guides, note pages, video, etc.), which may or may not have been referenced during the presentation.

Equipment: The Government will provide a projector and projector screen, and laptop for the Offeror to utilize in support of the Offeror's Oral Presentation. During the designated presentation time, the Government will make available, the Offeror's submitted Power Point Presentation, which was submitted as part of the Offeror's Written Proposal. No internet access will be available.

FACTOR 1: MANAGEMENT & TECHNICAL APPROACH

The Offeror shall provide a Management/Technical Approach describing how it will achieve quality results in managing the Task Order. The Quoter shall provide specific examples related to each of the technical prompts provided below. The Management /Technical approach shall focus at a minimum on, but is not limited to the following technical prompts:

1) **The Secure Flight program is ever evolving. What is the offeror's approach to support operations of the Secure Flight Operations Center (SOC) to include User Acceptance Testing (UAT) and implementation of process improvements for the SOC (SOW Section 3.1.1.1)?**

2) What is the offeror's approach to support interaction with airlines to support Secure Flight's Industry Performance Analysis (IPA), the conduct of interface testing between Secure Flight and the airlines, airline readiness assessment, On Boarding and Production Cutover (SOW Section 3.2)?

3) What is the offeror's approach to support collecting Secure Flight system, SOC systems, and program performance data, analyzing that data and reporting to program leadership and government stakeholders on the Secure Flight program and system performance (SOW Section 3.2.3)?

4) What is the offeror's experience in providing support in the areas of change management; specifically communications, technical writing, document management, and training, and response to requests from GAO, Congress, the press, the public, and other government entities (SOW Sections 3.3; 3.3.1.; 3.3.2; 3.3.3) and how will the offeror provide support in these areas to the Secure Flight Program.

5) What is the offeror's experience in supporting Business Architecture, Process and Planning (BAPP) functional area in multiple disciplines such as: Business Exploration, Release Planning, Requirements Management, Operations Partner Management and Secure Flight Reporting (SOW Sections 3.4.1; 3.4.2; 3.4.3; 3.4.4 and 3.4.5) and how will the offeror provide support in these areas to the Secure Flight Program?

6) What is the offeror's approach to support the Technical Support and Reporting team with resources with the technical skills and expertise necessary to provide Root-cause analysis? (SOW Section 3.5)?

7) What is the offeror's approach to support the Performance Engineering team by providing resources with the technical expertise and skills necessary to perform sophisticated data analysis and modeling to provide the ability to convey complex information to non-technical decision makers (SOW Section 3.6)?

8) What is the offeror's approach to adhere to all Security, Personnel Requirements, and Privacy clauses outlined in the provisions of contract SOW?

FACTOR 2 – KEY PERSONNEL & STAFFING APPROACH

The Quoter's Staffing Approach shall address at a minimum, the following:

1) *Stoffing opprooch:* The Quoter shall provide a Staffing approach to include a list of labor categories, function of each labor category, and number of labor hours for each labor category. The Quoter shall describe any teaming (including subcontractor) arrangements and the percentage of work to be performed by the prime contractor.
2) *Key Personnel:* Offerors shall propose the Key Personnel as they see fit. Offerors shall clearly detail how the education and experience of each person demonstrates their ability to perform

the requirements of the corresponding Statement of Work. Information presented shall contain the following information at a minimum:

a) Name of individual proposed.
b) Education: Relevant degrees awarded and majors.
c) Length of time employed by Quoter.
d) Cumulative amount of time (years) and description of relevant experience as indicated by projects and/or assignments in which experience was gained relevant to the Key Personnel proposed.
e) Key attributes of the personnel that show they meet or exceed the specifications of the labor category identified.
f) What prior work and experience do they have with airline industry reservation systems, departure control systems, data communications, and passenger processing for flight departures

B. VOLUME 1 -WRITTEN RESPONSE

COVER LETTER – 1 Page Limit
Your Cover Letter shall include the following:

1) Solicitation Number and Solicitation Title
2) Contractor Name
3) DUNS Number
4) DHS TABSS Schedule Contract Number
5) Complete Business Mailing Address
6) Point(s) of Contact (Name, title, e-mail address, phone number)
7) Teaming Partners , Subcontractors, and/or Contractor Teaming Arrangements (CTA)
8) Other Pertinent Information

FACTOR 1 – MANAGEMENT AND TECHNICAL APPROACH
The Offeror shall provide 5 printed copies of the slides to be used by the Offeror in support of the Dral Presentation of Factor 1. This is due at the time of the oral presentation.

FACTOR 2 – KEY PERSONNEL & STAFFING APPROACH
The Offeror shall provide 5 copies of the slides to be used by the Offeror in support of the Oral Presentation of Factor 2. This is due at the time of the oral presentation.

The Offeror shall submit a Commitment Letter from each named Key Personnel stating that the named person intends on working in support of the identified Task Order if the Contractor is awarded the Task Order, and that the Key Person's information provided by the Offeror as part of the Oral Presentation is accurate.

The Staffing approach should provide the labor category and labor description, and number of hours allocated per labor category based on the offeror's description of a Full Time Equivalent

(FTE). Address the ability to realign personnel in response to changing/fluctuating workload. Address the ability to reach back to team members/subcontractors.

Staffing plan Template for Task Order —With Labor Rates:

Labor Category (LCAT)	Job Title or Position Description -ref (volume and page no.'s from staffing plan)	SOW Technical req./Task (para. no.'s)	If Key Personnel Resume (volume II and page no.'s)	Highest Education Level and Degree Achieved	Professional Certifications Attained	Proposed Hours (hrs) Per year

Template Instructions:

For each Contract Line Item Number (CLIN), Offeror shall create a labor template using the above sample as the acceptable format and--

1 - Add as many rows and or columns to the above template as necessary to show each employee or subcontractor who will perform the work stated in the RFP for the entire duration of the period of performance, including options. When a specific resource is known, enter that person's name and company affiliation and identify if they are key personnel. When individual's name is not known, enter "Vacant", the date the vacancy is to be filled using the format "mm/dd/yy", and one of the following codes: CL- individual's commitment letter in hand; SC – subcontractor's commitment letter in hand; AR – actively recruiting; AS – actively negotiating with a subcontractor; AR – actively recruiting.; WR – will recruit.

2 – For each position (named or vacant) enter required data (labor category, job title or job description, cross-reference to the statement of work indicating work effort(s) that person will perform, location of resume if a key person (enter "N/A" if not a key person), highest education grade and degree achieved, professional certifications attained, number of proposed hours for that individual for each year of the Task Order.).

3 – Add as many columns to the above template as necessary to show all of the option years covered by the entire period of performance (base year and all options).

C. VOLUME II FACTOR 3- PAST PERFORMANCE

COVER LETTER – 1 Page Limit

Your Cover Letter shall include the following:

1) **Solicitation Number and Solicitation Title**
2) **Contractor Name**
3) **DUNS Number**
4) **DHS TABSS Schedule Contract Number**
5) **Complete Business Mailing Address**
6) **Point(s) of Contact (Name, title, e-mail address, phone number)**
7) **Teaming Partners , Subcontractors, and/or Contractor Teaming Arrangements (CTA)**
8) **Other Pertinent Information**

The Offeror shall provide no more than three (3) past performance references from prior customers on Contracts or Task Orders (as a prime contractor or subcontractor) that involve work of the same size, scope, and complexity that is being solicited by the TSA in this TORFP. **The Offeror may submit no more than two past performance references for their subcontractors under this acquisition. In any event, no more than 3 past performance references may be submitted, and at least one of the three must address the Offeror's past performance as a prime or as a subcontractor.**

For the "Past Performance" portion of the offeror's proposal, the offeror shall identify the following information for each of the past performance references the TSA will receive.

- Name of Agency
- Contract number(s) and type;
- Name, phone number, and e-mail address of two (2) technical points of contact at the entity for which the contract was performed;
- Contracting Officer's name, phone number, and e-mail address;
- Contracting Officer's Representative name, phone number, and e-mail address;
- Total Contract Dollar Value;
- Period of performance;
- Scope of the Contract/Task Order;
- Explanation of relevancy to the current requirements being solicited;
- Describe the extent of subcontracting; and

Statements relative to performance: i.e., statements describing whether the contract(s) were completed on time, performed satisfactorily while conforming to contract terms and conditions and without degradation in performance or customer satisfaction and any applicable information on problems encountered during performance; Note: include severity of any quantity, delivery or cost problems in performing the contract and the corrective action taken and the effectiveness of the corrective action.

The TSA may contact those references during the evaluation process to verify relevant experience and level of performance. The TSA may, at its discretion, obtain and evaluate information from sources other than those provided by the Offeror.

D. VOLUME III FACTOR 4– PRICE/COST

The resulting IDIQ Order will be a Time & Materials order. Provide your firm's TABSS labor rates and categories that would be utilized for this task. The government anticipates a discount. TSA will not award a task order to an Offeror's whose price submission in response to this RFP exceeds its current contract pricing listed on the TABSS contract.

- The price submission at a minimum shall include:
  - Awarded TABSS Rates
  - Proposed Task Order Discount
  - Net Fully Loaded Labor Rates after the applied blanket discount

- A complete breakdown of your TABSS labor categories, labor rates, number of Full-Time-Employees, and number of labor hours for each CLIN in sufficient detail to allow the Government a good understanding of your planned technical approach as outlined in the Task Order SOW.

- A maximum of a 2% labor rate escalation shall be proposed for each subsequent 12 month ordering period

The resulting Task Order will be Time and Materials. No adjustment to the prices, except those allowed by the contracting officer, shall be allowed. In completing Section B of this TORFP, offerors shall ensure that all of Section B including all blanks and spaces are completed. Offerors' proposals must identify the rates in the underlying IDIQ DHS TABSS contract that constitute the basis for the proposed price (how the prices were derived) in Section B, including, as applicable, labor categories, labor rates, proposed hours, supporting materials (if any), and any other items that constitute the rationale and supporting data for the prices proposed in Section B. Offerors must identify any proposed discounts from the IDIQ DHS TABSS contract rates.

Note: While cost will not be assigned a rating during the evaluation, it is a criterion in the overall evaluation of quotations. Proposed pricing will be evaluated to determine whether they are necessary and reasonable for the conduct of the proposed task order, reflect a clear understanding of the requirements, and are consistent with the methods of performance described in the offeror's quotation. Best value, in regards to superior technical quotations, will determine at what proposed and realistic cost will TSA award the contractor

L.5. PAGE LIMITATION:

Volume I Oral Presentation – FACTOR 1 & 2 No page limit
Volume II –FACTOR 3- No page limit
Volume III- FACTOR 4-No page limit

The written response to this TORFP must be in three separate volumes *(I. Technical Content, II. Past Performonce ond III. Cost/Pricing ond Forms)* with a cover sheet giving a clear indication of the contents of each volume. The proposal text font will be Times New Roman or Calibri 12-point type on standard 8 ½ inch by 11-inch paper with margins of at least 1" at the top, bottom and both sides.

Please note that contents on both sides of the paper will be counted as 2 pages. Failure to fully adhere to the prescribed page and format restrictions may result in your firm's disqualification from the competition.

L.6. OTHER INFORMATION:

Cover Letter: The Contractor's company contact information (including Company name, Point of Contact, Email address, Phone / Fax, Address, DUNS number, and DHS TABSS contract number) must be clearly indicated in a cover letter to be included as part of offeror's proposal.

L.7. CLARIFICATIONS:

The Government intends to award without discussions, but the Government also reserves the right to have discussions. All requests for clarifications shall be submitted only via email to the Contract Specialist, Ms. Delisa Corbett @ Delisa.Corbett@dhs.gov no later than 2:00 pm EST on Wednesday July 9, 2014.

L.8. SUBMISSION OF OFFERS:

Offerors are required to submit their proposal via email to the Contract Specialist, Ms. Delisa Corbett @ Delisa.Corbett@dhs.gov . Email messages should contain HSTS02-14-R-OIA072 in the subject line. Offerors are cautioned to submit their proposal in either PDF or Microsoft Office Format. Email responses must be received by 11:00 am EST on Wednesday July 23, 2014.

L.9. PROPOSAL ACCEPTANCE PERIOD:

The acceptance period is 180 calendar days after receipt of proposal.

(END OF SECTION L)

Section M Evaluation Factors for Award

1. EVALUATION FACTORS FOR AWARD

A. The Government will award a Task Order resulting from this solicitation to the responsible offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors shall be used to evaluate offers:

(i) Technical and Management Approach;
(ii) Key Personnel and Staffing approach;
(iii) Past Performance; and
(iv) Price

B. The Government will determine the best value solution by utilizing the trade-off method. The trade-off method enables the Government to conduct an integrated assessment of both technical and cost/price elements in each proposal. The technical (non-price) evaluation factors (Technical and Management Approach, Key Personnel and Staffing Approach and Past Performance) are ranked in descending order of importance (Technical and Management Approach and Staffing approach are most important) and are significantly more important than the Price Factor. As proposals become more equal in their non-price factors, the price factor may become more equal to the non-price factors.

C. The Source Selection Official (SSO) may make a determination to award the Task Order to other than the highest technically-rated proposal, or other than the lowest evaluated cost/price proposal. The government intends to award based on initial proposals. The SSO may determine to make trade-offs between technical and cost/price factors, which may result in a determination that a superior technical solution merits a higher cost/price for that solution.

D. The following represent the factors which will be evaluated using adjectival ratings in making an award determination:

FACTOR 1 – MANAGEMENT & TECHNICAL APPROACH (Oral Presentation)

The Government will evaluate the Offeror's Management and Technical Approach based on the oral presentation and will evaluate the Offeror's response to each of the identified technical prompts to determine if the Offeror has proposed a sound technical approach that exhibits understanding of the complexity and magnitude of the requirement and likelihood that the Offeror will be successful in performance under the resultant Task Order. Performance risk associated with the proposed approach will be identified by the Government.

FACTOR 2 – KEY PERSONNEL & STAFFING APPROACH

1) The Government will evaluate each of the proposed Key Personnel's level of qualifications and degree of experience demonstrated in relation to the SOW.
2) The Government will evaluate the key attributes of that show they meet or exceed the specifications of the labor category identified.
3) The Government will evaluate The Offeror's Staffing approach will be evaluated to determine the Offeror's ability to provide key personnel and resources with the technical expertise and skills to implement the Offeror's approach and solution to meet Task Order requirements. The Staffing approach will also be evaluated by the Government to determine how the Offeror's approach demonstrates it knowledge, skills, and abilities to fulfill the solicitation's requirements in a realistic manner.

FACTOR 3- PAST PERFORMANCE

1) The Government will evaluate the degree to which the Offeror's (3) past performance references from prior customers on contracts (as a prime contractor or subcontractor) demonstrates ability to perform contract in a satisfactory manner with the ability to comply with performance schedules, including the completion of tasks, managing work assignments, and delivering quality products and services.
2) Relevance of Past Performance. In assessing relevance of past performance, the Government will consider relevant contracts as those contracts that are ongoing or completed within the last three (3) years having comparable level of size, scope, and complexity to the requirements of the RFQ Task Order.
3) Actual Performance. In assessing the actual performance the Government will consider the Offerors demonstrated or proven ability to meet performance requirements, effectively manage resources, and achieve customer satisfaction.

FACTOR 4- PRICE

1) The Offerors' proposed prices for the Base Year and all Option Years for this Task Order to determine if the proposed prices are fair and reasonable for the work proposed. All Items for this Task Order will be evaluated and summed to create a single "Total Evaluated Price" for each proposal evaluated. The Government reserves the right to reject a proposal in the event that the lack of balance in pricing poses an unacceptable risk to the Government.

Through evaluation an offeror may be removed from consideration when:

- Prices are deemed unfair, unreasonable, or unbalanced when compared to the level of effort proposed in the offerors staffing approach
- Bases of estimate do not reflect a clear understanding of the requirements or are inconsistent with the Offeror's proposed technical and management approach...

The proposal will be assess whether the proposed price is fair and reasonable by considering the appropriateness of labor categories, labor mix, skill levels, and level of effort.

The Government will evaluate the Offeror's proposed labor categories, labor rates, proposed hours, supporting materials (if any), and any other items that constitute the rationale and supporting data for the fixed prices proposed in Section B in accordance with the Offeror's DHS TABSS contract.

------END OF REQUEST FOR PROPOSAL-------

SECTION B SCHEDULE OF SERVICES AND PRICE

1. SECTION B.1 CLIN X0007(pages 3, 4, 6 and 8) **Q: For the base year and each of the option years the there are two separate CLINs for '*Technical Support and Reporting*' (X005 and X007). Can the government please clarify the purpose for each CLIN?**

RESPONSE: CLIN "X"0007 hos been corrected to reflect Project Monogement & Reporting ond Requirements as described in SECTION C.2.4.

2. SECTION B.1 **Q: There is no separate CLIN for a program manager. Can the government confirm it is acceptable to provide a program manager with appropriate hours and responsibilities in all applicable CLINs?**

RESPONSE: The Government confirms thot the Offerors sholl identify o progrom monoger role with the oppropriote hours ond responsibilities in oll opplicoble CLINs.

3. SECTION B.1 OPTION YEAR-FFP (pages 5, 6 and 8) **Q: The RFQ includes a CLIN for 'Business Operations Support' for the option years, but not for the base year. Can the government please clarify the intended purpose of this CLIN and the difference in requirements in the option years?**

RESPONSE: The intended purpose of all OPTION YEAR –FFP CLINs is to allow the contract type to chonge from T&M to FFP, these CLINs will be exercised if the Government finds that it is in the best interest to convert this requirement from a Time-and-Materials contract to Firm Fixed Price upon determination of exercising the Option periods. Essentially, these Option Year CLINs completely replace the T&M optional CLINs - no base year CLIN for this purpose is necessory.

4. **Today we believe there are a total of 25.5 FTEs supporting the program;**

   2.5 supporting PMO functions,5 supporting BAPP,5 supporting OPT,6 supporting C&R,4 supporting IPA,3 supporting TS&R/PE; Can the government confirm that all these functions/support is considered part of this scope? Can the government also confirm this is the current level of effort?

RESPONSE: The functions/support areos above are considered port of this scope. While the Government will not specify the current level of effort, the estimote cited above for contractors is not correct. TSA considers the number af FTEs to be driven significantly by the lobar mix and the opproach proposed.

SECTION C STATEMENT OF WORK (SOW)

SECTION C 3.3 Communications and Readiness:

5. **What is the total number of end users that will require training?**

RESPONSE: There ore opproximotely 1,000 troining participonts per yeor (e.g. if on individual ottended 3 troining events, that individual occounts for 3 of the 1,000).

6. **What is the total number of stakeholders?**

RESPONSE: Stakeholders include approximotely: 260 airlines, ten government agencies, ten major internal TSA offices, four oirline industry associotions, Congressional members, and an unknown number of the public.

7. **What is the breakdown of audiences- i.e., organizations? (is there a matrix?)**

RESPONSE: Stakeholders include opproximately: 260 airlines, ten government agencies, ten major internal TSA offices, four oirline industry ossociotions, Congressionol members, ond on unknown number of the public.

8. **How many training locations are currently being utilized?**

RESPONSE: There is one primory troining locotion ot Annopolis Junction, Morylond; troining is occosionolly but infrequently conducted ot: o) Colorodo Springs, Colorodo, b) Arlington, Virginio, c) other locations in the Washington DC areo.

9. **What is involved with new hire training?**

    a. **How often?**

RESPONSE: New hire troining hos been conducted, on overoge, 15 times per yeor.

    b. **How many people?**

RESPONSE: New hire training hos been conducted, on overoge, for 150 porticiponts per yeor.

    c. **How long?**

RESPONSE: The new hire training is 2-to-3 days per sessian.

    d. **Delivery method- all instructor led? Some CBT?**

RESPONSE: All new hire training is delivered by instructor led sessians.

10. **Is there a current/preferred tool to develop computer based training?**

RESPONSE: Articulote software is currently used to develap computer bosed training.

11. **Are current trainings being managed and hosted within TSA's Learning Management System?**

RESPONSE: Current troinings ore not being monoged ond hosted within TSA's Leorning Monogement System.

12. What does the current organization change management team look like?

a. How is it structured?

RESPONSE: Three contractors supporting one lead government employee.

b. Who would we be working with?

RESPONSE: All Secure Flight government employees and contractor personnel.

c. Who would we report to?

RESPONSE: There is a Communications and Readiness lead government employee.

d. What are the current pain points?

RESPONSE: This question is too broad.

13. Are we able to get existing stakeholder assessment document?

RESPONSE: TSA intends to make documents available after award to the incumbent.

14. : What existing technologies are used for communications?

RESPONSE: Normal office software such as the Microsoft Office suite and Adobe PDF.

15. What is the current process for disseminating communications to internal and external stakeholders? (i.e., travel agencies, trade associations, congress)

RESPONSE: A private web board is used to disseminate communications to the airlines. Direct communications via email and/or PowerPoint presentations are used for Congress, industry associations, and other stakeholders. Coordination of external communications is frequently required with other TSA offices such as Office of Strategic Communications and Public Affairs, Office of Security Policy and Industry Engagement, Global Strategies, and Office of the Chief Counsel.

16. Clarification: What support is necessary for visits, tours and demonstrations?

RESPONSE: Visits, tours and demonstrations occur approximately twice per month. Support is required to tailor standard PowerPoint presentations for the specific visitor.

17. What does the training organization look like today?

RESPONSE: One lead government employee and three support contractors.

18. What is the In-The-Know Initiative Awareness Program for Vetting Operations Division?

RESPONSE: The In-The-Know Initiative Awareness Program is a presentation series designed to inform Vetting Operations Division employees and contractors about various TSA initiatives/programs. Topics are presented by Subject Matter Experts that are directly involved with the topic.

19. **Is there a current career development assessment tool?**

RESPONSE: At this time, there is no current career development assessment tool covered under the scope of this effort.

20. **Based on the request for workforce and employee development, there will be a significant need for secure flight resource support and engagement. Do we understand the government's ability to provide resources to support? (e.g., development of career development roadmaps is a work-intensive effort requiring knowledge only held by secure flight resources.)**

RESPONSE: Subject Matter Experts will be made available to provide insight to knowledge only held by Secure Flight resources.

21. **How does Secure Flight staff currently use TIDE (Terrorist Identities Datamart Environment)**

RESPDNSE: TSA reserves the right not to address this questian.

22. **Is there a dedicated training environment for training development?**

RESPONSE: Yes, there is a training room ot Annapolis Junction, Marylond with PCs for the individuol student and other support equipment.

23. **Is there a current performance-based training process?**

RESPONSE: No.

SECTION C.3.4 Business Architecture, Process, and Planning:

24. **What is the current size of the BAPP team?**

RESPONSE: The BAPP team currently consists of seven Government personnel and seven contractors.

25. **SDW 3.4 Business Architecture, Process, and Planning: "BAPP is responsible for ensuring that all requirements are traced to system use cases" - Are we responsible for developing use cases?**

RESPONSE: Pleose see section 3.4 in the Stotement of Work

26. **SOW 3.4.1 Business Exploration: Do we have access to Secure Flight's high-level strategic goals?**

RESPONSE: TSA intends to make documents available after oword to the incumbent.

27. **Do we have access to the Secure Flight Concept of Operations document?**

RESPONSE: TSA intends to make documents available after award to the incumbent.

28. What is the New Idea Capture process?

RESPONSE: The New Idea Capture process is as follaws. Thraugh continuous stakehalder develapment and exploratian, BAPP works with internal and external stakeholders to understand their current and future needs. BAPP provides the New Idea Form (NIF) to stakeholders to use as a means of documenting the high-level requirements far a new idea, concept ar capability. The BAPP team member representing the specific stakeholder grouping will offer support for completion of the form, as needed, and facilitate the forwarding of the NIF to the Requirements Manager.

29. What is the expectation for "assist to ensure proper impact assessment for change requests"?

RESPONSE: BAPP consults with the System Development and Testing organizotion to ossist in determining the level of complexity/effort for copabilities considered within o chonge request.

30. What requirements management tool is currently being used (i.e., Rational)?

RESPONSE: Rational RequisitePro

31. What are the as-is activities/relationships with the SF operational partners?

RESPONSE: Coordination for the requirements of technical interfaces ond operational procedures between Secure Flight and the operotionol portner.

32. What reporting tool is currently being used?

RESPONSE: Tools primarily include Oracle Business Intelligence reporting tools, Informatica, and Microsoft Excel.

SECTION L- INSTRUCTIONS, CONDITIONS AND NOTICES

SECTION L.3.A (table, page 49) under the staffing approach refers to the "staffing approach spread sheet," "the Section B Table" and the "Staffing plan template."

33. Q: Are these the same documents as described on pages 53 and 54.

RESPONSE: No. the SECTION B toble description is found on poges 2-8 which are identified as the CLINS. The Staffing plon template is described on poges 53-54. These ore seporote table thot must be completed as part of the written submission.

34. Q: If not, can the government provide instructions on how offerors should complete each of these documents?

RESPONSE: The SECTION B table must be completed to show the overoll proposed price for each CLIN for eoch period of performance excluding the OPTION YEAR-FFP CLINs. The Staffing plon template must be

completed to show labor category, technical requirement/task they will be warking an as described in SECTION C, natation if they are key personnel, level of educotian, certifications, and praposed haurs for the base year for assigned task.

35. Are these documents to be provided in the slides or in a separate volume?

RESPONSE: Bath tables will be submitted as part of Volume III- Cost/Pricing. The staffing plan shauld additionally be presented in the Oral presentation Volume II factor 2.

SECTION L.A.3.H(page 49) "All information submitted in response to this solicitation, inclusive of graphics, shall be formatted on 8 ½" x 11" size paper, use 12-point sized font, single line spacing, and 1-inch margins. Tables, figures and graphs may use 9 point font. All pages must be numbered."

SECTION L.4 (page 56) "The proposal text font will be Times New Roman 12-point type on standard 8 ½ inch by 11-inch paper with margins of at least 1" at the top, bottom and both sides."

36. May offerors use fonts other than Times New Roman in the orals presentation?

RESPONSE: Offerors must use Times New Raman and Calibri as acceptable fonts.

37. May offerors use fonts other than Times New Roman in the written volume (past performance and resumes)

RESPONSE: Written proposal text font will be Times New Roman or Calibri only.

38. Are presentation slides exempt from the 1-inch margin requirement?

RESPONSE: Oral Presentation slides are exempt fram all format specifications other than font type and size.

39. May offerors use 9-point font in tables, figures and graphs in the oral presentation, resumes, and past performance volume?

RESPONSE: Resumes and the Past Performance volume must adhere ta the 12- point font.

40. Do these instructions apply only to the past performance document or to the presentation slides as well?

RESPONSE: Instructians for the aral presentations have been changed ta remave specifications other than font type and size.

41. Could the government please verify that the slide presentations are due in a PowerPoint file format along with the written response?

RESPONSE: The slide presentations will only be accepted in PowerPoint file format. The written response may be submitted in Microsoft Word or Adobe PDF format.

42. **For presentations, how will contractors be allowed to access their presentation? Will the slide deck be provided from what is submitted to the government via email, or is it necessary for the contractor to bring the presentation on a zip drive, CD, etc.?**

RESPONSE: SECTION L.4.A Equipment states" that the Government will make available the submitted PowerPoint presentation, which was submitted as part of the Offerors written proposal. No internet access will be available."

43. **For the written submission, must bidders provide two separate presentation decks (one for Factor 1, and a second for Factor 2)? Or can this be one combined presentation deck as long as bidders clearly address both factors?**

RESPONSE: The slide presentation may be submitted as a combined presentation deck, but the Factors must be clearly divided.

44. **Is it acceptable for the final printed copies of the oral presentation to be printed in color?**

RESPONSE: Yes

45. **Could the government please verify that the slide presentations are due in a PowerPoint file format along with the written response?**

RESPONSE: Yes. Please see SECTION L.8 SUBMISSION OF OFFERS

46. **During the 90 minute presentation, will there be a break between the 60 and 30 minute sessions, or will it be one continuous session?**

RESPONSE: The presentation will be one continuous session.

47. **Per the RFP page 50, bidders are given 90 minutes total for delivery of their proposal. Are bidders able to use the 90 minutes as they see fit, or must bidders follow the time structure listed on page 48 which allots 60 minutes for Management/Technical and 30 minutes for Staffing?**

RESPONSE: The Offeror may determine how to use the allocated time; TSA has removed the structure.

48. **Given the complexities associated with an orals presentation proposal, will the government provide a two-week extension to the written proposal due date and similarly push the anticipated presentation delivery dates out two weeks? Thus making written proposals due on 8/6/14 and oral presentations planned for the week of 8/18/14?**

RESPONSE: No extension will be given.

49. **The government has specified that the number of offeror attendees for the oral presentation is limited to four (4) people. Given the diversity of skillsets required to execute the program, will the government consider increasing the total number of attendees to 6 to provide better inclusion of key representatives?**

RESPONSE: TSA will allow no more than 6 people from each Offeror to attendee the orol presentation.

50. **Management & Technical Approach' requests: "The Secure Flight program is ever evolving. What is the offeror's approach to support operations of the Secure Flight Operations Center (SOC) to include User Acceptance Testing (UAT) implementation of process improvements for the SOC (SOW Section 3.1.1.1)?" Can the government please clarify if UAT and implementation of process improvements are to be handled distinctly (e.g., "UAT *and* implementation of process improvements").**

RESPONSE: UAT is separate from the "implementation of process improvements".

51. **Is it acceptable to submit subcontractor past performances in addition to those submitted by the Prime? If so, how many must be from the Prime?**

RESPONSE: The Offeror may submit no more than 3 past performance references. No more than two (2) past performance references for their subcontractors under this acquisition will be accepted.

SECTION M Evaluation Factors for Award

52. On Page 57 of the RFP, Section M Evaluation Factors for Award – Could the Government provide information regarding the rating scale the Government will use to evaluate each non-price factor (e.g., adjectival ratings)?

RESPONSE: TSA will be using adjectival ratings for all non-price factors.

END OF QUESTIONS

SECTION C- STATEMENT OF WORK (SOW)

C.1.1 REQUIRING ORGANIZATION

U. S. Department of Homeland Security, Transportation Security Administration (TSA), Office of Intelligence & Analysis (OIA)

C.1.2 BACKGROUND

To enhance the security of air travel, the Secure Flight program assumed the responsibility for the passenger watch list matching functions, previously performed by aircraft operators. Secure Flight improves aviation security by identifying known and suspected terrorists and distinguishing them from the remainder of the traveling population. Based on this analysis, TSA can more effectively allocate screening resources to focus efforts on potential terrorist threats.

Secure Flight supports TSA's effort to implement intelligence-driven, risk-based screening procedures such as TSA Pre-Check. Secure Flight identifies high-and low-risk passengers in order to mitigate known and unknown threats to aviation security and designate them for enhanced screening, expedited screening, or prohibition from boarding a covered flight, as appropriate. The Secure Flight program enhances the security of domestic and international commercial air travel, by prescreening more than two million aircraft passengers a day.

C.1.3 SCOPE OF WORK

The contractor shall perform the full range of Functional Category Domain 1: Program Management, Engineering and Technology Support Services functions for ongoing Secure Flight operations and maintenance support within the following functional areas: *Optimization, Industry Performance and Analysis (IPA), Communications and Readiness (C&R), Business Architecture, Policy and Planning, Technical Support and Reporting (TS&R), and Performance Engineering PE)*. The contractor shall provide a full and adequate range of support services that meet the SOW requirements.

C.2 TECHNICAL REQUIREMENTS/TASKS

3.1 Optimization

3.1.1 Secure Flight Operations Center (SOC)

Secure Flight houses an operations center to conduct manual review of near matches to watch lists and for facilitating discussions between airlines and Secure Flight regarding inhibited passengers. The airline is required to receive government approval for the passenger to board their flight. In order for airlines to permit passengers who are potential matches to board their flight, the airline needs to contact the SOC and provide additional identity information to clear the passenger.

3.1.1.1 Implementation of Enhancements for Secure Flight Operations Center

The contractor shall provide SOC resources to develop content for system User Acceptance Testing (UAT) - user interface, case management, and knowledge management applications, quality assurance planning and other system and functional requirements. The contractor will also draft and upon

government approval, execute UAT scenarios, support training requirements for the SOC, assist in the reconfiguration of existing facilities and equipment based on new program populations and analyze the impact on SOC design and requirements, and support testing of all SOC systems including user interfaces based on system requirements and functionality.

3.1.1.2 Operations and Maintenance for Secure Flight Operations Center

Working in both classified and unclassified environments, the contractor shall provide assistance with process assessment/improvement, reporting refinement, workforce modeling, strategy, quality assessment, vetting logic/analysis, interoperability and interaction with non-Secure Flight operations, and knowledge management maintenance.

NOTE: Work within the entire Optimization area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.2 Industry Performance and Analysis (IPA)

IPA is a joint contractor and Government team responsible for onboarding airlines to Secure Flight, improving technical compliance in accordance with the Consolidated Users Guide (CUG), providing assistance in bringing new populations to Secure Flight (e.g. 12.5 carriers), and ensuring active carrier compliance with new requirements (e.g. Risk Based Security). In order to achieve these goals, a phased deployment approach has been developed and successfully implemented. The approach includes Aircraft Operator Interface Testing, Assessment, On Boarding and Production Cutover.

- Aircraft Operator Interface Testing consists of the execution of test cases to validate aircraft operator system functions and interfaces. During this phase of deployment, Secure Flight and the aircraft operators will conduct connectivity testing and system to system testing.
- After all aircraft operator interface testing is complete TSA will evaluate the test results to determine the capabilities of the aircraft operator to prepare for the next phase of deployment.
- Dn-boarding begins after the aircraft operator assessment is complete. The aircraft operator submits production passenger data to Secure Flight but the aircraft operator does not apply the boarding pass printing results at this time. Qualitative watch list matching analysis occurs during this phase and is a comparison analysis of current airline system matching results with the Secure Flight matching system. Qualitative watch list matching analysis provides the program with current aircraft operator matching results to engineer the Secure Flight system to minimize the false positive rate.
- The last phase of deployment is production cutover where the aircraft operator submits production passenger data, the Secure Flight watch list matching system processes the data and sends a boarding pass printing instruction to the aircraft operator. The aircraft operator must begin using the boarding pass printing instruction.
- After the airline has cutover to using the Secure Flight system, the contractor (with oversight from Government team members) will continually review data analysis (See Dperational Performance) with the airlines to improve system performance. They will evaluate airline data submission performance for compliance with the Secure Flight rule and system requirements.

3.2.1 Continue Airline Deployments

The contractor will support the IPA team by providing operational and technical guidance in airline

operations, system testing and system implementation strategy. This will include drafting test strategies, test plans, airline system implementation procedures and reference material for airline guidance, and maintaining the Airline Operator Data Base (AODB). To be successful, the contractor will require individuals to be subject matter experts in airline operations and system testing. The contractor will assist the IPA team in coordinating connectivity, system testing and the cutover of aircraft operator watch list matching to the Secure Flight program.

3.2.2 Operations and Maintenance for IPA

The contractor will support IPA in analyzing carrier data submissions to determine root causes, develop performance improvement plans, and assist air carriers and their respective service providers to make improvements so that their Secure Flight data submissions are made in full compliance with the Consolidated User Guide (CUG). Additionally, the contractor will provide technical expertise and guidance to the Secure Flight team to ensure Secure Flight technical systems are functioning properly with the aircraft operators.

Additionally, the contractor will provide support to the Compliance Monitoring group within IPA to assist in the evaluation of carrier behavior, develop compliance packages for use by the Office of Security Operations (OSO) and Office of Global Strategies (OGS), and form recommendations for carrier performance improvement.

3.2.3 Performance Data

IPA is responsible for collecting Secure Flight system, SOC systems, and program performance data, analyzing that data and reporting to program leadership and government stakeholders on the Secure Flight program and system performance. The program has identified over 100 performance measures that will identify system and user performance. Users include but are not limited to the airlines, SOC staff and other government stakeholders to be defined. Examples of performance measures identified so far include:

- Secure Flight System - Number of Transmissions Received, False Positive Rate, Submission Volumes by Airline, System Response Time to Airline, and System Outage.
- SOC - Manual Reviews, Selectee and No Fly Notification reports, Average Hold Time, Average Handle Time, Call Type, and Calls Handled.

3.3 Communications and Readiness

The contractor shall provide support in the areas of change management, specifically drafting communications, technical writing, document management, and training. Specific examples of work, which will be performed by the contractor, may include but not limited to:

3.3.1 Communications

- Maintain the Secure Flight Change Management (CM) Plan and associated work to include assessing current situation; develop/maintain change management strategy. The CM Plan should include CM goals and high-level activities to be supported.
- Update and maintain existing Stakeholder Assessment document.

- Maintain a comprehensive Communications and Stakeholder Outreach Plan to include, but not limited to, audience, delivery techniques to include new and existing technologies, i.e. (classroom, videoconference, webinar, etc.,), timing, frequency, key messages, communications methodology, approval processes, stakeholder satisfaction, strategy, scorecard, and feedback mechanisms.
- Maintain a list of current and approved frequently asked questions and answers.
- Develop, coordinate, and disseminate informational material for various internal and external stakeholders of Secure Flight including but not limited to Government Accounting Office, Office of Inspector General, and other agencies/departments.
- Draft informational content for press releases, public affairs guidance, and website posting and routinely review the information for irrelevant or outdated content.
- Draft and upon government approval, issue informational material on the Secure Flight Program to internal and external stakeholders (aircraft operators, travel agencies, trade associations, congress, GAO, the press etc.). Informational material will be in various forms including, but not limited to meeting content, newsletters, presentations, toolkits, job aids, correspondence, and letters.
- Support Secure Flight Program senior leadership by drafting presentations, talking points, and briefings materials.
- Provide critical analysis of information to assist in the development of accurate Secure Flight Program communications products
- Assist in building strong partnerships within Secure Flight and OIA to increase effectiveness and awareness of communications products and requirements.
- Draft and upon government approval, update and distribute Communications Standard Operating Procedures (SOP).
- Provide support to coordinate, manage and execute all aspects of aviation industry conferences.
- Draft, coordinate and disseminate periodic Secure Flight Program Newsletters.
- Support Secure Flight Program visits, tours, and demonstrations.
- Review and provide Secure Flight comment and coordination on externally produced documents.
- Archive communication products on TSA's IShare site for easy identification and retrieval.
- Assist in drafting and coordination of responses to requests for information from Congress and TSA or DHS leadership.
- Assist OIA and other offices with communications support and review of products pertaining to the Secure Flight Program.
- Additional Stakeholder Communications as required.

3.3.2 Technical Writing and Document Management

- Provide quality assurance of program communication products which are produced under section 3.5 in this SOW.
- Maintain and update the Secure Flight Style Guide, the Secure Flight glossary, and the Secure
- Flight Acronym List.

- Support key document and vital records library semi-annual reviews and updates.

3.3.3 Training

- Conduct training needs assessments for various Secure Flight entities.
- Draft training plan and training materials for Vetting Operations Division as outcome from the training needs assessments.
- Draft, maintain and refine New Hire Training course materials, transitioning appropriate modules to blended learning approach including a computer-based training.
- Deliver instructor-led courses.
    - Draft and deliver system course materials for all Secure Flight System Releases and new operational technologies based on release schedule.
    - Assist in analysis of new program initiatives to determine training requirements.
    - Propose training delivery methods and program initiated course materials to support the rollout of new features, population and capabilities based on pilot and go-live dates.
- Propose, coordinate, and facilitate Domain and Initiative Awareness programs (In-the-Know) for Vetting Operations Division.
- Draft appropriate job aids to support external stakeholders.
- Support resource management and efficiency efforts by identifying and instituting standardized training processes and tools.
- Workforce Development/Employee Development:
    - Support personnel career development by identifying appropriate training and professional development opportunities in the areas of: training opportunity awareness, curriculum development, and supervisor support.
    - Draft an employee development plan for Vetting Operations Division.
    - Draft career-progression roadmaps for non-intelligence analysts.
    - Draft a job rotation and Vetting Operations Division-level, cross-training program.
    - Support Skills Gap Analysis for employees or team to identify competency (knowledge, skills, and abilities) gaps.
    - Draft a training catalog that can be posted on IShare and maintained, available for staff to develop one-stop-shop to address performance gaps.
- Draft a database-training plan (e.g. Terrorist Identities Datamart Environment -TIDE, etc.) coordinated with other agencies and vendors.
- Draft communications on training offered by DHS/TSA/OIA and others.
- Draft performance-based process training guidance – repository of training opportunities based on performance feedback.
- Draft a "cohort" training approach that would bring supervisors from different branches together in collaborative sessions.
- Draft supervisor toolkits.

NOTE: Work within the Training area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.4 Business Architecture, Process, and Planning

The Business Architecture, Process and Planning (BAPP) functional area currently supports multiple disciplines such as: updating and maintaining current Secure Flight business process model flows and updating and maintaining current requirements in business requirements matrices and other requirement artifacts. BAPP is responsible for ensuring that all requirements are traced to system uses cases and must work closely with the Technology Solutions Division to ensure all requirements are properly implemented. The contractor will perform the following work:

3.4.1 Business Exploration

- Propose and/or draft new business processes that could streamline or support the Secure Flight business model.
- Assist in the translation of Secure Flight high-level strategic goals into business requirements.
- Support the coordination of business requirements and use cases with impacted stakeholders. Ensure deployed systems meet business requirements. Ensure User Acceptance Testing (UAT) and Validation adequately address business goals, objectives, and requirements.
- Draft concept definition papers and business cases as necessary.
- Support Secure Flight business analysts to identify and improve common business practices and ensure standardization across the Secure Flight Program and the Vetting Operations Division.
- Manage the updates and change processes related to the Secure Flight Concept of Operations (ConOps) document in alignment with the Department of Homeland Security's Strategic Plan, establish Secure Flight Program external governance plans, related processes and documentation.
- Support business continuity planning to assist the Secure Flight program; including subject matter expertise in planning and designing business continuity planning for all of the business areas of the Secure Flight program.

3.4.2 Release Planning

- Support the capture, sponsorship, and prioritization of requirements and changes for future release iterations through management of the New Idea Capture process and the Business Change Board.
- Assist to ensure proper impact assessment for change requests.
- Maintain the Program roadmap and capability prioritization pipeline.
- Support with the Technology Solutions Division to determine Secure Flight release milestones.
- Support the development and management of each release plan.

3.4.3 Requirements Management

- Draft and, upon government approval, manage business-centric requirements deliverables within each release, including documentation and validation of requirements tracing.
- Draft Business Requirement Matrices, Problem Reports (PRs) for requirements, and other requirements management artifacts, as needed (e.g. Business Architecture Document and Business Requirement Documents).
- Support business validation for tracing:

  - Business requirements to Standard Operating Procedures (SOPs)
  - Business requirements to system use cases.
  - System use cases to test plans.
  - Test plans to test results.
- Support and coordinate User Acceptance Testing (UAT) across the program.
- Log requirements and related artifacts into Secure Flight repository tools.
- Support implementation of business and operational requirements development and management processes.
- Establish mechanisms for business transition planning and management capability to ensure clear communication within the Secure Flight Program and with stakeholders. Coordinate efforts with organizational change management and ensure a smooth transition from the current state to the desired state.

3.4.4 Operational Partners Management

Support the management of relationship and coordination activities with Secure Flight operational partners, including:

- TSA Transportation Security Redress Branch (TSRB);
- TSA Office of Risk Based Security (ORBS);
- Customs and Boarder Projection (CBP); and
- Department of Justice's (DOJ's) Terrorist Screening Center (TSC).
- Assist with the documentation of operational partner agreements including Memoranda of Understanding (MOUs), Inter- and Intra- Agency Agreements (IAAs), Inter- and Intra-Departmental Agreements (IDAs), Interface Control Documents (ICDs), Service Level Agreements (SLAs), and others as needed.

3.4.5 Secure Flight Reporting

The contractor shall assist with managing the Secure Flight Reporting mailbox, including:

- Analyzing reporting data requests and confirming requirements with stakeholders.
- Researching data to satisfy requests, using available analytic tools.
- Coordinating with other teams such as Technology Support and Reporting to fulfill requests.
- Performing quality assurance on outgoing Secure Flight Reporting data and content.
- Performing ongoing stakeholder management in areas such as data quality and interpretation.
- Developing and maintaining Secure Flight Reporting SOPs.
- Collaborating with other BAPP team members to recommend and implement Business Change Requests (BCRs) resulting from Secure Flight Reporting work.
- Recommending and implementing operational process improvements, as needed.

NOTE: Work within the entire Business Architecture, Process, and Planning area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.5 Technical Support and Reporting

The contractor will support the Technical Support and Reporting team by providing resources with the technical expertise necessary to provide support for the various Secure Flight subsystems. Knowledge of the specific Secure Flight subsystems will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Data management
- Report development using Oracle Business Intelligence Enterprise Edition (OBIEE)
- Data analysis
- Root-cause analysis

3.6 Performance Engineering

The contractor will support the Performance Engineering team by providing resources with the technical expertise necessary to perform sophisticated data analysis and modeling. Knowledge of specific Secure Flight data will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Statistical data analysis
- Data extraction and manipulation (requires extensive SQL and some programming knowledge)
- Ability to convey complex information to non-technical decision makers (data visualization)
- Mathematical modeling for impact and predictive analysis
- Ability to devise processes to evaluate a closed source system

4. Project Management & Reporting and Requirements

The contractor shall perform project management services and resources required for performance under this SOW. The contractor shall comply with existing OIA and/or program- specific Configuration Management processes and procedures for hardware, software, and documentation. Specific requirements include but are not limited to:

- Contractor Work Breakdown Structure (CWBS)
- Cost, Schedule, Forecast and Performance Reporting
- Ad Hoc Reports

The contractor shall provide project management data within the monthly report, as identified in section 4.2 below.

4.1 Work Breakdown Structure

The contractor shall provide a resource-loaded contractor work breakdown structure (CWBS), outlining the proposed activities, resources and costs to complete the requirements of this SOW. This CWBS shall align seamlessly into, and reflect the respective work outlined in the Government- provided Integrated Master Schedule (IMS).

The draft resource-loaded CWBS shall be provided to the Government for approval within 10 working

days of the start of this Task Order Period of Performance. The CWBS will list the work activities, duration of each task/activity, resources required, deliverables, and cost for each work activity to be performed. This shall be the baseline CWBS, against which progress will be measured. The CO and Task Order COR. must approve any deviation from this baseline. The contractor shall report based upon a resource-loaded CWBS for schedule and requirements tracking that is proposed by the contractor and approved by the government.

4.2 Monthly Report

The contractor shall provide a monthly report outlining the contractor's cost, schedule and performance for the project by Task Order.

The contractor shall provide contractor performance reports that show the status of the contractor's production and performance assessment against the expected performance goals. Reports should show the following at a minimum:

- Reporting period
- Progress/Status
- Current month's activities (broken out to tasks performed for each effort/activity with resource assigned)
- Percentage of completion
- Forecast of next month's activities
- Issues encountered and any corrective actions during the reporting period
- Funding to date
- Cumulative dollar and percentage of funds expended
- Total funds remaining
- Projected spending for next month
- Total projected Task Order costs
- Funding shortfall date (if applicable)
- Hours expended per resource

A draft monthly reporting format will be presented to the government for approval within fourteen (14) calendar days of the start of the Period of Performance of this Task Order. The monthly report shall be submitted to the COR at least three (3) business days prior to the Program Management Review (PMR) meeting.

4.3 Ad Hoc Reports

An Ad Hoc report is a report requested by the Program Business Functional Manager addressing an area of concern not listed as a formal deliverable.

4.4 Travel

The contractor will be reimbursed for reasonable and actual costs for transportation, lodging, and meals and incidental expenses in accordance with Federal Travel Regulations (FTR). Travel performed for

personal convenience or daily travel to and from work at the contractor's facility or local government facility (i.e., designated work site) shall not be reimbursed. Prior to undertaking any travel other than local, the contractor shall submit a request for specific approval to the COR, listing names of individuals traveling and destinations, dates, purpose and estimated cost of the trip. The contractor will use the Travel Authorization form for all travel conducted. All requests for travel must be pre-approved by the government business functional lead and the COR, and must contain the information required on the Travel Request Form (see TSA IShare), to include an estimated amount not to exceed expenses consistent with Joint Travel Regulations and GSA per diem schedules.

4.5 PMR Meeting

The contractor shall conduct Monthly Program Management Reviews to present to the government information on project status to include: Performance measurements, progress towards completion, associated risks, issues and cost. The information shall be provided with summary and appropriate details of status and projected performance in the following areas: Functional performance and progress, project risks and mitigation progress, establish logical and realistic corrective action plan(s) to address identified issues, and establish priorities for execution based on the criticality of identified issue(s). Any issues identified during this review that need resolution shall be recorded and tracked by the contractor in an Action Item database. The status and disposition of all open action items shall be presented at the program review meeting, noting that disposition of each action item requires approval of the appropriate government representative - Project Manager (PM), Task Order COR, or CO. The contractor shall minimize resources and costs in connection with the monthly PMR meetings. The contractor shall conduct meetings before the fifteenth (15^{th}) business day of the month, unless otherwise directed by the government.

5. Deliverables

The following table describes the Contract Data Requirements List (CDRLs) that are required for this SOW. The Contractor requires express written approval from the CO before executing any change to the scope, content, and/or delivery schedule of the described work products and tasks in this SOW.

Table 1: Contract Data Requirements List

CDRL #	Deliverable	Description	Frequency	Reference
001	User Acceptance Testing (UAT) Analysis	Plan User Acceptance Testing Efforts: Evaluate User Acceptance Testing Results, identify system enhancements and recommend changes to improve operating efficiencies	Based on each release (estimated Quarterly)	SOW Sections 3.1.1.1 and 3.4.3
002	Parallel Testing Guidance	Write testing guides and procedures for the parallel testing phase of implementation	Update as needed	SOW Section 3.2.1

003	Parallel Testing Analysis	Create parallel testing analysis and report	As specified by airline implementation plans	SOW Section 3.2.1
004	Cutover Strategy and Criteria Plan	Write and develop airline cutover strategy and monitor individual airline cutover schedule compliance	As needed, to align with implementation of new Airline Operators	SOW Section 3.2.1
005	Cutover Readiness Review	Summarize cutover readiness for each Airline Operator	Weekly	SOW Section 3.2.1
006	Airline Operator Test Reports	Detailed results of onboard testing for each Airline Operator	At the conclusion of each Airline Operator's onboarding	SOW Section 3.2.1
007	Operational Readiness Test Plan	Write testing guides and procedures for the operational readiness testing phase of implementation	Update as needed	SOW Section 3.2.1
008	Consolidated User Guide (CUG)	Enhance/modify the Consolidated User Guide (CUG)	Update as needed	SOW Section 3.2.1
009	Secure Flight Style Guide, Acronym List, and Glossary	Maintain the Secure Flight style manual (guide), acronym list, and glossary	Quarterly updates as needed. Final Assessment Due at end of TO	SOW Section 3.3.2
010	Secure Flight Comprehensive Training Plan	Maintain comprehensive training plan which outlines objectives, needs, strategy, timelines and curriculum for Vetting Operations Division training	Annual updates as needed. Final Assessment Due at end of TO	SOW Section 3.3.3
011	Training Materials	Create/maintain training material detailed in the Secure Flight training plan	As specified in the Secure Flight Training Plan	SOW Section 3.3.3
012	Workforce Development/ Employee Development	Create/maintain employee development initiatives as identified in the employee development plan	Quarterly Submission of artifacts created. Annual updates as needed	SOW Section 3.3.3

013	Secure Flight Business Architecture	Modifications and/or enhancements to Secure Flight business requirements and business process model/flows	Due per functionality/project implementation and release (estimated Quarterly) Ad Hoc Emergency Process Change Requests	SOW Section 3.4.3
014	Ad-hoc and recurring reports	Various reports to transmit Secure Flight data to stakeholders to inform decision-making	Create as needed	SOW Sections 3.2.3, 3.5 and 3.6
015	Contractor Work Breakdown 5tructure (CWB5)	Resource-loaded schedule, including cost, performance, and requirements tracking that the Contractor proposes and is approved by the Government for each Task Order. The CWB5 contains scheduled work products and related services for each mission application and align with the program's IMS (if provided)	10 Working Days after Task Order issued, updates as needed	SOW Section 4.1
016	Monthly Report	Cost, Schedule, and Performance Report	Draft: Within 14 calendar days of the start of the Period of Performance of each Task Order Monthly: no later than 10th Business day of	SOW Section 4.2
017	Program Management Reviews (PMRs)	Monthly meeting to discuss 5chedule, Costs, Resources, Technical issues, problems and resolutions	No later than the 15th Business Day of each month	5OW Section 4.5
018	Final Report	Summarizes support activities, “start to completion schedules”, deliverables and results achieved relative to the performance objectives of this SOW	Draft report 15 working days prior to conclusion of work. Final report 5 working days after receipt of comments	SOW 5ection 5

019	Firm Fixed Price Proposal & SOW	Detailed Scope of Work with tasks breakdown and deliverables identified	No later than 90 days before execution of exercising the Option Period	SOW Section B.2

The dates shown in the Deliverables Table are the required initial delivery date, which initiates the government acceptance timeline described below. All plans and documents are intended to provide continuity with previous work performed and to provide a comprehensive set of program management guidance and reporting as well as systems development and management documentation.

All deliverables, existing plans and documents shall be used in their current form where applicable and shall be updated as appropriate to accommodate deficiencies, program and development changes. Documents listed but not currently existing shall be created and delivered at the time specified in the frequency column above. The contractor shall prepare and maintain all documentation in accordance with an industry standard best practice for auditable, repeatable engineering process to assure the availability and accuracy of a comprehensive, complete, and current set of plans, reports, and documents.

The contractor shall use the TSA Systems Development Life Cycle Guidance Document, version 2.0, (or updated version) for updating of systems development documentation form and content.
The list of documents and their content and format may be refined and tailored by mutual agreement between the government and contractor to assure quality program management, systems development, and systems operation and management. The contractor shall also use the TSA Style Guide when preparing all deliverables. The Style Guide can be found on the TSA intranet at:

http://tsaweb.tsa.dot.gov/tsaweb/intraweb/assetlibrary/web_best_practices_and_style_guide.pdf

(END OF SECTION C)

SECTION D - PACKAGING AND MARKING

D.1 Markings

All deliverables submitted to the TO Contracting Officer or the TO Contracting Officer Representative (COR) shall be accompanied by a packing list or other suitable shipping documentation that shall clearly indicate the following:
(a) Contract number;
(b) Task order number;
(c) Name and address of the consignor;
(d) Name and address of the consignee;
(e) Government bill of lading number covering the shipment (if any); and
(f) Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).

(END OF SECTION D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

All contract deliverables, including documents and system implementations, require approval and formal acceptance by the Task Order COR. The Government will have up to 10 business days after receipt of a deliverable to accept or reject any deliverable. If the Task Order COR rejects a deliverable, the Contractor will be provided specific written comments detailing the basis for the rejection and recommended corrective action. The Contractor shall have up to 10 calendar days to address all specific written comments by either incorporating the requested Government changes or providing an explanation of why the Government-requested changes are not being incorporated. The Government will have an additional five (5) calendar days to review and provide a final decision regarding acceptance or rejection of the deliverable.

E.2 Scope of Inspection

Documents submitted by the Contractor shall be professional in content and presentation according to commonly accepted standards of writing and editing in the subject field. The Contractor shall provide electronic copies to the Government Program Manager, Task Order COR, Contracting Officer and any other specified Government representatives as directed by the Government when due. All documents shall be delivered in Microsoft Office format (including Word, Excel, PowerPoint, Access, Visio, and Project) or other formats accepted by the government by direction of the Task Order COR. Previously released documentation will be delivered in current format unless mutually agreed otherwise.

E.3 Basis of Acceptance

Final CDRL deliveries shall be accompanied with a letter of delivery and Government acceptance to be signed by the Task Order COR and Project Manager (PM).

E.4 Review of Deliverables

At any point in the process of the review of deliverables, the deliverable is considered accepted if the Government provides written acceptance or does not provide comments and/or change requests within fifteen (15) business days of the receipt of the deliverable.

E.5 Final Deliverables

The contractor shall provide two (2) Compact Disk- Read Only Memory (CD-ROM) copies of the set of all final documents at the end of each Task Order. All documents shall be delivered in a format mutually agreed to between the contractor and the government. Previously released documentation will be delivered in current format unless mutually agreed otherwise. CDRL content may be combined into one delivered document with notification.

(End of Section E)

SECTION F- PERFORMANCE

F.1 PERIOD OF PERFORMANCE

The period of performance for this task order will be for a base period of twelve (12) months from award date with two (2) 12 month option periods and one (1) seven month option period to end June 21, 2018. The period of performance will start upon all contractor personnel's completion of TSA's personnel security process and deemed suitable/eligible to start work.

F.2 PLACE OF PERFORMANCE

Contractor's personnel will work full-time during core hours (0800-1800) at TSA Annapolis Junction location. Frequent visits to TSA Headquarters location may be necessary in some circumstances and will be coordinated and approved by the COR and the contractor Program Manager. The contractor is expected to provide on-site support during this timeframe on an 8-hour per day, 5-day a week basis.

U.S. Department of Homeland Security
Transportation Security Administration
132 National Business Parkway
Annapolis Junction, MD 20701

F.3 GOVERNMENT FURNISHED FACILITIES

The Government identifies the following GFE and GFI for this effort:

- Use of Government-provided facilities for contractor office space;
- Computer-hosting facilities with appropriate power, space and environment;
- Operating environments to include a workstation;
- Documentation required for facility and system accreditation;
- OIA On/Off-boarding procedures and;
- Access to TSA's Online Learning Center (OLC) – TSA's automated training system used to meet the mandated privacy and security training requirements.
- Necessary access to the TSA Intranet (internal website) and related software tools
- Access to copier and duplicating equipment

F.4 TRAVEL REQUIREMENTS

Long distance Travel is required in support of this Task Order. The Government will reimburse travel in accordance with the Federal Travel Regulations. All travel must be pre-approved by the COR.
Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed.

(END OF SECTION F)

SECTION G- CONTRACT ADMINISTRATION DATA

G.1. CONTRACTING OFFICER (CO)

The Contracting Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue orders, obligate funds and authorize the expenditure of funds, and notwithstanding any term contained elsewhere in this contract, such authority remains vested solely in the Contracting Officer. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) In the event, the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:
NAME: Joseph Wolfinger
PHONE NUMBER: 571-227-2429
EMAIL: Gloria.Uria@tsa.dhs.gov

G.2. CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COR) AND TECHNICAL MONITORS

1. The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

2. The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

TSA CDR:
NAME: Anthony Pinto
PHONE NUMBER: 240-568-5307
EMAIL: Anthony.Pinto@tsa.dhs.gov

3. The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

4. The responsibilities and limitations of the COR are as follows:
   - The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
   - The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
   - The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
   - The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
   - The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
   - The COR is not authorized to direct the Contractor on how to perform the work.
   - The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
   - The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

5. The responsibilities and limitations of the TM are as follows:
   - Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.
   - Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
   - Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
   - Informing the COR if the Contractor is not meeting performance, cost, and schedule milestones.
   - Performing technical reviews of the Contractor's proposals as directed by the COR.
   - Performing acceptance of the Contractor's deliverables as directed by the COR.
   - Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

G.3 SUBMISSION OF INVOICES

(a) Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

(b) Invoice Submission Method: Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:
1) Facsimile number is: 757-413-7314

The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (e) of this clause.

2) U.S. Mail:
United States Coast Guard Finance Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake, VA 23327-4111

3) Email Invoices:
FIN-SMB-TSAInvoices@uscg.mil or
www.fincen.uscg.mil

(c) Invoice Process: Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Technical Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

(d) Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

(1) Via the internet: https://www.fincen.uscg.mil
Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

(2) Via the Payment Inquiry Form: https://www.fincen.uscg.mil/secure/payment.htm

(e) Invoice Elements: Invoices will automatically be rejected if the information required in subparagraph (a) (2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and DUNS number are not included in the invoice. All invoices must be clearly correlate invoiced amounts to the corresponding contract line item number and funding citation.

(f) Supplemental Invoice Documentation: Contractors shall submit all supplemental invoice documentation (e.g. copies of certified time sheets (as applicable), subcontractor invoices, receipts, signed receiving reports, travel vouchers, etc) necessary to approve an invoice along with the original

invoice. The Contractor invoice shall contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Invoice charges shall be billed per appropriate Contract Line item Number (CLIN), period of performance and obligated funding. Unless otherwise authorized by fiscal law, funding from one CLIN may not be utilized to offset charges on another CLIN, specifically if it is different accounting and appropriation data. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Technical Representative.

(h) Frequency of Invoice Submission: Invoices may be submitted on a bi-weekly or monthly basis. Once the invoicing method has been chosen, this method shall be the frequency of invoicing for the life of the Task Order.

(END OF SECTION G)

SECTION H- SPECIAL REQUIREMENTS

H.1 DISCLOSURE OF INFORMATION

Information furnished by the Contractor under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personally-identifiable information must be clearly marked.
Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the requirements of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.
In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and information and must ensure that all work performed by its Subcontractor(s) shall be under the supervision of the Contractor or the Contractor's employees.

H.2 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION

Publicity releases in connection with this contract shall not be made by the Contractor unless prior written approval has been received from the Contracting Officer.
The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.
A minimum of five full business days' notice is required for requests made in accordance with this provision.

H.3 CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES

If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

H.4 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.
(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.5 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

The T5A may enter into contractual agreements with other Contractors (i.e., —Associate Contractors) in order to fulfill requirements separate from the work to be performed under this contract, yet having a relationship to performance under this contract. It is expected that contractors working under TSA contracts will have to work together under certain conditions in order to achieve a common solution for T5A. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant Contracting Officer (CO) and/or designated representative in providing suitable, non-conflicting technical and/or management interface and in avoidance of duplication of effort. Information on

deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.
Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant CO and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.
Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a —lead Contractor for the project. In these cases the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.
Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

H.6 NON-PERSONAL SERVICES

—Personal services are those in which contractor personnel would appear to be, in effect, Government employees via the direct supervision and oversight by Government employees. No personal services shall be performed under this contract. No Contractor employee will be directly supervised by a Government employee. All individual Contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor of the Contractor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.
The Contractor shall not perform any inherently governmental actions as defined by FAR 7.500. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change any contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.
The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this clause. Nothing in this special contract requirement shall limit the Government's rights in any way under any other term of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this special contract requirement shall be included in all subcontracts at any tier.

H.7 CONTRACTOR RESPONSIBILITIES

The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.
The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government

and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.
A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition.
The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall not:
Discuss with unauthorized persons any information obtained in the performance of work under this contract. Conduct business not directly related to this contract on Government premises.
Use computer systems and/or other Government facilities for company or personal business other than work related; or
Recruit on Government premises or otherwise act to disrupt official Government business.

H.8 QUALIFICATIONS OF EMPLOYEES

The Contracting Officer may require dismissal from work under this contract and/or removal of access to government facilities, property, information and/or information systems of those employees which the Contracting Officer deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment the Contracting Officer deems contrary to the public interest or inconsistent with the best interest of national security.

H.9 NON-DISCLOSURE AGREEMENTS

Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive But Unclassified, Government procurement sensitive information, and/or other sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

H.10 OBSERVANCE OF LEGAL HOLIDAYS

The Government observes the following holidays:

New Year's Day	*Martin Luther King Birthday*
President's Day	*Memorial Day*
Independence Day	*Labor Doy, Columbus Day*
Veteran's Doy	*Thanksgiving Day*
Christmas Day	*Inauguration Doy (Washington, DC metropolitan area)*

In addition to the days designated as holidays, the Government observes also the following days:
Any other day designoted by Federal Stotute,
Any other day designoted by Executive Drder, and
Any other day designoted by President's Proclamation.

Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be

reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Technical Representative.
In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursable and time and material (T&M) contracts, the government will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.
Otherwise, the management responsibility for contractor functions approved by the Contracting Officer for offsite work, in the event of inaccessibility of federal workplaces are the sole responsibility of the contractor. The contractor may propose telework or other solutions when critical work is required, however, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location and all resources necessary to complete such performance.
In the event of an actual emergency, the Contracting Officer may direct the contractor to change work hours or locations or institute tele-work, utilize personal protective equipment or other mandated items.

H.11 ADVERTISING OF AWARD

The contractor shall not refer to contract awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

H.12 MAJOR BREACH OF SAFETY OR SECURITY

(a) Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Safety is essential to TSA and compliance with safety standards and practices is a material part of this contract. A major breach of safety may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of safety must be related directly to the work on the agreement. A major breach of safety is an act or omission of the Contractor that consists of an accident, incident, or exposure resulting in a fatality, serious injury, or mission failure; or in damage to equipment or property equal to or greater than $1 million; or in any "willful" or "repeat" violation cited by the Occupational Safety and Health Administration (OSHA) or by a state agency operating under an OSHA approved plan.

(b) Security is the condition of safeguarding against espionage, sabotage, crime (including computer crime), or attack. A major breach of security may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of security may occur on or off Government

installations, but must be related directly to the work on the agreement. A major breach of security is an act or omission by the Contractor that results in compromise of classified information or sensitive security information or sensitive but unclassified information, including contractor proprietary information, illegal technology transfer, workplace violence resulting in criminal conviction, sabotage, compromise or denial of information technology services, equipment or property damage from vandalism greater than $250,000, or theft greater than $250,000.

NOTE: Breach of Security for the purposes of this definition should not be confused with breach of security in screening operations.

(c) In the event of a major breach of safety or security, the Contractor shall report the breach to the Contracting Officer. If directed by the Contracting Officer, the Contractor shall conduct its own investigation and report the results to the Government. The Contractor shall cooperate with the Government investigation, if conducted.

H.13 CONTRACTOR STAFF TRAINING

The contractor shall provide fully trained and experienced personnel. Training of contractor personnel shall be performed by the contractor at its expense, except as directed by the Government through written authorization by the Contracting Officer to meet special requirements peculiar to the contract. Training includes attendance at seminars, symposia or user group conferences. Training will not be authorized for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer languages and computer operating systems that are available on the commercial market or required by a contract. This includes training to obtain or increase proficiency in word processing, spreadsheets, presentations, and electronic mail.

H.14 EMPLOYEE TERMINATION

The contractor shall notify the Contracting Officer immediately whenever an employee performing work under this contract who has been granted access to government information, information systems, property, or government facilities access terminates employment. The contractor shall be responsible for returning, or ensuring that employees return, all DHS/TSA -issued contractor/employee identification, all other TSA or DHS property, and any security access cards to Government offices issued by a landlord of commercial space.

H.15 STANDARDS OF CONDUCT AND RESTRICTIONS

The contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. Personnel performing work under this contract shall not:
Solicit new business while performing work under the contract;
Conduct business other than that which is covered by this contract during periods paid by the Government;

Conduct business not directly related to this contract on Government premises; Use Government computer systems or networks, and/or other Government facilities for company or personal business; Recruit on Government premises or otherwise act to disrupt official Government business.

H.16 ELECTRONIC AND INFORMATION TECHNOLOGY TO ACCOMMODATE USERS WITH DISABILITIES (SECTION 508 OF THE REHABILITATION ACT)

Section 508 of the Rehabilitation Act prohibits federal agencies from procuring, developing, maintaining, or using electronic and information technology (EIT) that is inaccessible to people with disabilities. The applicable standards in Section 508 of the Rehabilitation Act, as amended, shall apply to this contract and any items, or services covered by or provided in connection with this requirement. The Contractor shall provide items and services that comply with Section 508 requirements and the Electronic and Information Accessibility Standards at 36 CFR Part 1194.

H.17 WORKPLACE VIOLENCE PREVENTION

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be required to complete Workplace Violence Prevention training available through the TSA Online Learning Center. The course, entitled "Preventing Workplace Violence at TSA" shall be completed within 60 days of onboarding.

H.18 NOTIFICATION OF PERSONNEL CHANGES

The Contractor shall notify the Contracting Officer's Technical Representative (COR) in writing of any changes needed in building, information systems, or other information access requirements for its employees in order to meet contract requirements not later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to the COR: full name, social security number, effective date, and reason for change.

H.19 SUBSTITUTION OF KEY PERSONNEL

The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract's requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

(a) an explanation of the circumstances necessitating the substitution;

(b) a complete resume of the proposed substitute; and

(c) any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

H.20 CONTROLLED UNCLASSIFIED INFORMATION DATA PRIVACY AND PROTECTION

The Contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the Government ii) Government data transmitted by the contractor, and iii) Government 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 Government data, including but not limited to Personal Identifiable Information (PII), Sensitive Security Information (SSI), and Sensitive But Unclassified (SBU), and/or Critical Infrastructure Information (CII), shall be protected according to Department of Homeland Security information security policies and mandates.
At the expiration of the contract, the contractor shall return all Government information and IT resources provided to the contractor during the contract.
The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow all applicable DHS Component Agency's requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI, Informational Security and Privacy training, if required by the DHS Component Agency
The Contractor, and those operating on its behalf, shall adhere to the requirements of the non-disclosure agreement unless authorized in writing by the Contracting Officer.
The Government will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment as applicable. If encryption is required, the following methods are acceptable for encrypting sensitive information:

a. Products Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

The contractor shall maintain data control according to the applicable DHS Component Agency's security level of the data. Data separation will 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 must comply with TSA MD 3700.4 if applicable.
Users of Government 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 Government IT assets are expected to actively apply the practices specified in the TSA Information Technology Security Policy (ITSP) Handbook, Chapter 3, Section 6, Privacy and Acceptable Use, or similar DHS Component Agency's guidance or policy.
The contractor shall comply with the all data disposition requirements stated in the applicable DHS Component Agency's Information Security Policy. For all TSA orders the contractor shall comply with Information Security Policy Handbook Chapter 3, Section 17 Computer Data Storage Disposition, as well as TSA Management Directive 3700.4.

H.21 PERSONNEL ACCESS

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be subject to the security procedures set forth in this contract.

H.22 SUITABILITY DETERMINATION FOR CONTRACTOR EMPLOYEES

All contractor employees seeking to provide services to TSA under a TSA contract are subject to a suitability determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Office of Security, Personnel Security Division (PerSec), will allow a contractor employee to commence work on a TSA

contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

A suitability determination involves the following three phases:

Phase 1: Enter On Duty Suitability Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination will include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final suitability determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed suitable to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Technical Representative (COTR) of the favorable determination. Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for final suitability adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

Phase 3: Final Suitability Adjudication: TSA PerSec will complete the final suitability determination after receipt, review, and adjudication of the completed OPM background investigation. The final suitability determination is an assessment made by TSA PerSec to determine whether there is reasonable expectation that the continued employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final suitability determination will result in a notification to the COTR that the contractor employee has been deemed unsuitable for continued contract employment and that he/she shall be removed from the TSA contract.

H.23 SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE

(a) Definitions.

—Breach (may be used interchangeably with —Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any

similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.
—Personally Identifiable Information (PII) as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.
Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII) as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:
Driver's license number, passport number, or truncated SSN (such as last 4 digits)
Date of birth (month, day, and year)
Citizenship or immigration status
Financial information such as account numbers or Electronic Funds Transfer Information Medical Information
System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)
Other Personally Identifiable information may be —sensitive depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.
Sensitive PII have higher impact ratings for purposes of privacy incident handling.
(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding its systems, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.
(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4
In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;
(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements
(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
(6) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
(i) Authorized and official use;
(ii) Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;
(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.
(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.
The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.
(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.
(f) Personally Identifiable Information Notification Requirement. The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.
In the event that a PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.
(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

H.24 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 all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 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 non-disclosure 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 Technical Representative (COTR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

H.25 Contract Status Review

a. Background. Prompt, accurate data gathering, analysis and reporting enables both the Contractor and the Government to make sound decisions relating to performance under the contract. While the Contractor is solely responsible for performance, the Government wishes to be informed on all actions under the contract that affect compliance with contract cost, performance or schedule compliance.

b. Reporting Content. The Contractor shall provide information according to the slides included in the Contractor In-Process Status Review template that is attached to this contract. A matrix describing each slide and its reporting requirements follows:

Slide title	Deliverables
Requirement for contractor's reporting	The contractor shall identify each major deliverable under the contract and identify the required delivery date and those activities that the contractor has identified as critical to meet that delivery date

Slide title	Schedule
Requirement for contractor's reporting	The contractor shall report each item under the contract's schedule with the planned and actual dates for deliveries identified.

Slide title	Upcoming Events
Requirement for contractor's reporting	The contractor shall identify significant upcoming events as planned under or related to the contract that relate to contract performance.

Slide title	Human Resources/Staffing
Requirement for contractor's reporting	The contractor should include the elements as listed on the slide, with particular attention devoted to the extent to which the key personnel identified under the contract (by their positions) are actually filled and performing or what exact activities are underway to hire suitable candidates for performance.

Slide title	Risks
Requirement for contractor's reporting	The contractor shall report each risk area earlier identified (a red or yellow status item, anticipated cost overrun or late deliverable) and provide an assessment of the risks to the contract performance if the item is not capable of being remedied in time to attain the required contract performance.

Slide title	If Firm-Fixed Price
Requirement for contractor's reporting	The contractor should discuss delivery schedule compliance.

c. Reporting Method. The Contractor shall convene a meeting, located at the mutual convenience of the Contractor and Government that will include the Contractor's principal managers directing contract performance in which to explain the information presented in the attached slides. All persons identified as contractor "key personnel" in the attached contract will present the information contained in or related to their particular area of the contract status reporting template. The Government's Contracting Officer, Contracting Officer's Technical Representative, the Program Manager and other relevant Government personnel will attend. The Contractor should be able both to present information called for on the slide templates as well as questions from the Government related to them. During the course of the contract, this status reporting process is expected to generate action items for the contractor to address, and the status and progress of resolving each action item must be addressed at each meeting.

d. Reporting Frequency. The Contractor shall report the template information on a quarterly basis. The contractor shall deliver a copy of the final prepared charts for the required briefing to the COTR and Contracting Officer not later than two business days prior to the scheduled meeting.

e. Additional Requirements. The Government may, at its discretion, require additional items to be reported through the course of the contract and will provide additional instructions concerning such.

f. The effort required gathering data, report such, and conduct the required reporting process is included in the total price of this contract, and no activity related to these required status reports will be available for any further adjustment under the contract.

H.26 5200.225.001 Notice to Offerors/Contractors Concerning Trade Agreements terms applicability to the Transportation Security Administration (APR 2014)

With respect to the following Federal Acquisition Regulation (FAR) provisions and clauses listed directly below:

FAR 52.225-1 "Buy American Act—Supplies,"
FAR 52.225-2 "Buy American Act-Certificate,"
FAR 52.225-5 "Trade Agreements,"
FAR 52.225-6 "Trade Agreements Certificate,"
FAR 52.225-9 "Buy American Act—Construction Materials,"
FAR 52.225-10 "Notice of Buy American Act Requirement-Construction Materials,"
FAR 52.225-11 "Buy American Act—Construction Materials under Trade Agreements," and FAR 52.225-12, "Notice of Buy American Act Requirement—Construction Materials under Trade Agreements"

Offerors are hereby notified that the World Trade Organization Government Procurement Agreement presently makes the Transportation Security Administration (TSA) subject only to sources from within the following signatory countries: Canada, Chinese Taipei, Hong Kong, Israel, Liechtenstein, Norway, European Union, Iceland, and Singapore. Otherwise, the only other trade agreements that presently cover the TSA are the North American Free Trade Agreement and the U.S.-Chile Free Trade Agreement. The TSA cannot evaluate offers or award contracts to sources from countries not covered in these identified trade agreements or as specified herein. Offerors must analyze their intended proposals and provide information in response to the required provisions accordingly.

The European Union participation is as defined at
http://www.wto.org/english/thewto_e/countries_e/european_communities_e.htm

H.27 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.
(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.28 TECHNICAL INSTRUCTION

(a) Performance of the work described herein may be subject to written or oral technical instructions issued by the Contracting Officer's Representative specified in Section 11.2 of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "Changes" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.
(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.
(d) Failure of the Contractor and the CO to agree on whether Government direction is technical direction or a Change within the purview of the "Changes" clause shall be a dispute concerning a question of fact within the meaning of the Clause of the General Provision entitled, "Disputes."
(e) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

H.29 5200.231.001 TRAVEL AND PER DIEM (APPLICABLE TO COST REIMBURSEMENT AND T&M TYPE CONTRACTS ONLY) (AUG 2013)

The Contractor shall be reimbursed for travel costs associated with this contract. The reimbursement for those costs shall be as follows:

- Travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.
- Per diem will be reimbursed, at actual costs, not to exceed, the per diem rates set forth in the Federal Travel Regulations prescribed by General Services Administration and when applicable, Standardized Regulations Section 925 – Maximum Travel Per Diem Allowances for Foreign Areas – prescribed by the Department of State.
- Travel of more than 10 hours, but less than 24 hours, when no lodging is required, per diem shall be one-half of the Meals and Incidental Expenses (M&IE) rate applicable to the locations of temporary duty assignment. If more than one temporary duty point is involved, the allowance of one-half of the M&IE rate is prescribed for the location where the majority of the time is spent performing official business. The per diem allowance shall not be allowed when the period of official travel is 10 hours or less during the same calendar day.
- Airfare costs in excess of the lowest rate available, offered during normal business hours are not reimbursable.
- All reimbursable Contractor travel shall be authorized through the issuance of a task order executed by the Contracting Officer.

Local Travel Costs will not be reimbursed under the following circumstances:

- Travel at Government installations where Government transportation is available
- Travel performed for personal convenience/errands, including commuting to and from work; and

- Travel costs incurred in the replacement of personnel when such replacement is accomplished for the Contractor's or employee's convenience.

H. 30 5201.242.001 PERIOD OF PERFORMANCE FOR CONTRACTS REQUIRING EMPLOYEE BACKGROUND CHECKS (AUG 2013)

The period of performance begins 60 days after contract award to allow for the Enter On Duty Suitability Determination. A contract modification shall be executed to revise the period of performance if the determination process is completed earlier.

The following restricts shall apply to this contract:

1. The Contractor will access classified material at the following TSA facilities: Annapolis Junction- 132 National Business Parkway , Annapolis MD 20701 and TSA Headquarters -702 12th Street South, Arlington VA 22202

2. All contractor personnel assigned to this contract shall possess security clearances issued by the DSS commensurate with the level of required access to classified information that is directly in support of this contract. To perform on this contract, contractor personnel must possess a Secret security clearance, while others will be assigned to designated roles requiring access to Top Secret/Sensitive Compartmented Information (SCI). Those contractor personnel requiring access to SCI must be eligible under the provisions of Intelligence Community Directive (ICD) 704 without exception.

3. All contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access. If approved for access, contractor personnel will receive an indoctrination briefing by TSA Special Security Office (SSO) security staff prior to being granted access to SCI. All personnel security reporting requirements of ICD 704 will be made directly to the TSA SSO. Prior to leaving this contract, personnel will be scheduled for debriefing with the TSA SSO.

4. If required, the Contractor must store and safeguard SCI material in accordance with the applicable DCIDS or ICDs. Additionally, collaterally classified information (Confidential, Secret, and Top Secret) must be safeguarded, in accordance with DHS Instruction 121-01-011, "The DHS Administrative Security Program," and the Department of Defense (DOD) Manual 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM) for Safeguarding Classified Information." Additionally, the contractor must obtain prior written approval from the contracting officer or Contracting Officer Technical Representative (COTR) before executing NISPOM Chapter 5, Section 5-502, which authorizes the contractor to disclose classified information to cleared subcontractors. Further, NISPOM Chapter 5, Section 5-506, restricts the contractor from disclosing classified information received or generated under this TSA contract to any other Federal agency unless prior authorized is granted the Program office or contracting office. In accordance with the NISPOM, Chapter 5, Section 5-509, the contractor shall not disclose

classified information to another contractor except to support a contract, subcontract or other TSA purpose.

5. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

6. SCI will not be released to contractor employees without specific approval of the originator of the material as outlined in governing directives and based on prior DHS approval and certification of their need-to-know. Inquiries pertaining to classification guidance and safeguarding procedures for SCI generated under this contract will be directed to the responsible Special Security Officer (SSO).

7. SCI provided in support of this contract remains the property of DHS or its component agency originator. Upon completion or cancellation of the contract, SCI materials will be returned to the direct custody of the responsible SSO, or destroyed in accordance with instructions outlined by the Contracting Officer.

(END OF SECTION H)

SECTION I- ADDITIONAL CLAUSES

The terms and conditions of the DHS TABSS Schedule shall govern with the following FAR and HSAR clauses that are either incorporated by reference or provided in full text herein. The complete text can be found at http://farsite.hill.af.mil/farsite_alt.html and click on current FAR and HSAR then select the appropriate clause.

I.1 52.204-1 APPROVAL OF CONTRACT (DEC 1989)

This contract is subject to the written approval of the Contracting Officer and shall not be binding until so approved.
(End of clause)

I.2 52.204-2 SECURITY REQUIREMENTS (AUG 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."
(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

I.3 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in section 31.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Department of Homeland Security
Transportation Security Administration
Office of Acquisition TSA-25
Attn: Gloria Uria
601 South 12th Street Arlington, VA 20598-6025

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(END OF SECTION I)

SECTION J- ATTACHMENTS

J-1	Non- Disclosure Agreement (to be executed on date of award)
J-2	SSI Cover Sheet
J-3	DD 254

(END OF SECTION J)

End of Task Order

SECTION C- STATEMENT OF WORK (SOW)

1.1. C.1.1 REQUIRING ORGANIZATION

U. S. Department of Homeland Security, Transportation Security Administration (TSA), Office of Intelligence & Analysis (OIA).

C.1.2 BACKGROUND

To enhance the security of air travel, the Secure Flight program assumed the responsibility for the passenger watch list matching functions, previously performed by aircraft operators. Secure Flight improves aviation security by identifying known and suspected terrorists and distinguishing them from the remainder of the traveling population. Based on this analysis, TSA can more effectively allocate screening resources to focus efforts on potential terrorist threats.

Secure Flight supports TSA's effort to implement intelligence-driven, risk-based screening procedures such as TSA Pre-Check. Secure Flight identifies high-and low-risk passengers in order to mitigate known and unknown threats to aviation security and designate them for enhanced screening, expedited screening, or prohibition from boarding a covered flight, as appropriate. The Secure Flight program enhances the security of domestic and international commercial air travel, by prescreening more than two million aircraft passengers a day.

C.1.3 SCOPE OF WORK

The contractor shall perform the full range of Functional Category Domain 1: Program Management, Engineering and Technology Support Services functions for ongoing Secure Flight operations and maintenance support within the following functional areas: Optimization, Industry Performance and Analysis (IPA), Communications and Readiness (C&R), Business Architecture, Policy and Planning, Technical Support and Reporting (TS&R), and Performance Engineering PE). The contractor shall provide a full and adequate range of support services that meet the SOW requirements.

C.2 TECHNICAL REQUIREMENTS/TASKS

3.1 Optimization

3.1.1 Secure Flight Operations Center (SOC)

Secure Flight houses an operations center to conduct manual review of near matches to watch lists and for facilitating discussions between airlines and Secure Flight regarding inhibited passengers. The airline is required to receive government approval for the passenger to board their flight. In order for airlines to permit passengers who are potential matches to board their flight, the airline needs to contact the SOC and provide additional identity information to clear the passenger.

3.1.1.1 Implementation of Enhancements for Secure Flight Operations Center

The contractor shall provide SOC resources to develop content for system User Acceptance Testing (UAT) - user interface, case management, and knowledge management applications, quality assurance planning and other system and functional requirements. The contractor will also draft and upon government approval, execute UAT scenarios, support training requirements for the SOC, assist in the

reconfiguration of existing facilities and equipment based on new program populations and analyze the impact on SOC design and requirements, and support testing of all SOC systems including user interfaces based on system requirements and functionality.

The contractor shall coordinate with the appropriate business and technical organizations to promote operationally valuable enhancements and better satisfy end user requirements, to include, but not limited to:

- **Facilitating monthly or Government directed ad-hoc cross-functional and organization workshops**
- **Developing and enhancing user-specific training materials on an "as needed" basis**
- **Increasing communication channels**
- **Recommending modifications to the requirements and release management processes and products**

3.1.1.2 Operations and Maintenance for Secure Flight Operations Center

Working in both classified and unclassified environments, the contractor shall provide assistance with process assessment/improvement, reporting refinement, workforce modeling, strategy, quality assessment, vetting logic/analysis, interoperability and interaction with non-Secure Flight operations, and knowledge management maintenance.

The contractor shall support The Government in implementing improvements that will evolve the SOC into the National Transportation Vetting Center (NTVC). Tasks include, facilitating working sessions, developing transition plans and a viable operations model, establishing and/or modifying processes and products, and coordinating communication across multiple stakeholders. Support also includes coordinating closely with other OIA and TSA elements to properly communicate these transformational changes and incorporate relevant feedback. The contractor shall continue to support the continued on-boarding of new vetting populations and subsequent operational enhancements of the Secure Flight system.

NOTE: Work within the entire Optimization area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.2 Industry Performance and Analysis (IPA)

IPA is a joint contractor and Government team responsible for onboarding airlines to Secure Flight, improving technical compliance in accordance with the Consolidated Users Guide (CUG), providing assistance in bringing new populations to Secure Flight (e.g. 12.5 carriers), and ensuring active carrier compliance with new requirements (e.g. Risk Based Security). In order to achieve these goals, a phased deployment approach has been developed and successfully implemented. The approach includes Aircraft Operator Interface Testing, Assessment, On Boarding and Production Cutover.

- Aircraft Operator Interface Testing consists of the execution of test cases to validate aircraft operator system functions and interfaces. During this phase of deployment, Secure Flight and the aircraft operators will conduct connectivity testing and system to system testing.

- After all aircraft operator interface testing is complete TSA will evaluate the test results to determine the capabilities of the aircraft operator to prepare for the next phase of deployment.
- On-boarding begins after the aircraft operator assessment is complete. The aircraft operator submits production passenger data to Secure Flight but the aircraft operator does not apply the boarding pass printing results at this time. Qualitative watch list matching analysis occurs during this phase and is a comparison analysis of current airline system matching results with the Secure Flight matching system. Qualitative watch list matching analysis provides the program with current aircraft operator matching results to engineer the Secure Flight system to minimize the false positive rate.
- The last phase of deployment is production cutover where the aircraft operator submits production passenger data, the Secure Flight watch list matching system processes the data and sends a boarding pass printing instruction to the aircraft operator. The aircraft operator must begin using the boarding pass printing instruction.
- After the airline has cutover to using the Secure Flight system, the contractor (with oversight from Government team members) will continually review data analysis (See Operational Performance) with the airlines to improve system performance. They will evaluate airline data submission performance for compliance with the Secure Flight rule and system requirements.

3.2.1 Continue Airline Deployments

The contractor will support the IPA team by providing operational and technical guidance in airline operations, system testing and system implementation strategy. This will include drafting test strategies, test plans, airline system implementation procedures and reference material for airline guidance, and maintaining the Airline Operator Data Base (AODB). To be successful, the contractor will require individuals to be subject matter experts in airline operations and system testing. The contractor will assist the IPA team in coordinating connectivity, system testing and the cutover of aircraft operator watch list matching to the Secure Flight program.

3.2.2 Operations and Maintenance for IPA

The contractor will support IPA in analyzing carrier data submissions to determine root causes, develop performance improvement plans, and assist air carriers and their respective service providers to make improvements so that their Secure Flight data submissions are made in full compliance with the Consolidated User Guide (CUG). Additionally, the contractor will provide technical expertise and guidance to the Secure Flight team to ensure Secure Flight technical systems are functioning properly with the aircraft operators.

Examples of support that the contractor shall provide include:

- **Analyzing and incorporating submission timing and submission completeness into reports that support compliance activities and initiatives.**
- **Analyzing Visual Identification (VID) data and incorporating findings into reports that support compliance activities and initiatives.**
- **Preparation and presentation of carrier performance reviews that incorporate multiple factors.**

- **Coordinating and facilitating communications with carriers with respect to: answering carriers' questions, obtaining data, findings from analysis, etc.**
- **Performing other ad-hoc analysis as requested by field operations, analysts, and senior leadership to support decision making and/or other ongoing security initiatives.**

Additionally, the contractor will provide support to the Compliance Monitoring group within IPA to assist in the evaluation of carrier behavior, develop compliance packages for use by the Office of Security Operations (OSO) and Office of Global Strategies (OGS), and form recommendations for carrier performance improvement.

3.2.3 Performance Data

IPA is responsible for collecting Secure Flight system, SOC systems, and program performance data, analyzing that data and reporting to program leadership and government stakeholders on the Secure Flight program and system performance. The program has identified over 100 performance measures that will identify system and user performance. Users include but are not limited to the airlines, SOC staff and other government stakeholders to be defined. Examples of performance measures identified so far include:

- Secure Flight System - Number of Transmissions Received, False Positive Rate, Submission Volumes by Airline, System Response Time to Airline, and System Outage.
- SOC - Manual Reviews, Selectee and No Fly Notification reports, Average Hold Time, Average Handle Time, Call Type, and Calls Handled.

3.3 Communications and Readiness

The contractor shall provide support in the areas of change management, specifically drafting communications, technical writing, document management, and training. Specific examples of work, which will be performed by the contractor, may include but not limited to:

3.3.1 Communications

- **Develop, coordinate, execute, and** maintain the Secure Flight Change Management (CM) Plan and associated work to include assessing current situation; develop/maintain change management strategy. The CM Plan should include CM goals and high-level activities to be supported. **Change management activities include, but are not limited to:**
    - **Directly supporting senior Secure Flight and OIA leadership with their respective initiatives**
    - **Utilizing change management for Secure Flight and associated OIA initiatives**
    - **Creating comprehensive and robust change management strategies and plans**
    - **Using industry best practices to effect and maintain good change management practices**
    - **Planning and executing stakeholder assessments through interviews, focus groups, and other venues**
    - **Applying change management for the establishment and ongoing operational/maintenance (O&M) of the National Transportation Vetting Center**

    - **Applying change management for the establishment and O&M of branch-specific and/or cross-branch initiatives**
- Update and maintain existing Stakeholder Assessment document.
- Maintain a comprehensive Communications and Stakeholder Outreach Plan to include, but not limited to, audience, delivery techniques to include new and existing technologies, i.e. (classroom, videoconference, webinar, etc.,), timing, frequency, key messages, communications methodology, approval processes, stakeholder satisfaction, strategy, scorecard, and feedback mechanisms.
- Maintain a list of current and approved frequently asked questions and answers.
- Develop, coordinate, and disseminate informational material for various internal and external stakeholders of Secure Flight including but not limited to Government Accounting Office, Office of Inspector General, and other agencies/departments.
    - **Develop and execute strategic communications plans, to include :**
    - **Creating a comprehensive outreach campaign with respect to the establishment of the National Transportation Vetting Center (e.g., new product development, close coordination, communications infrastructure establishment, plan creation, stakeholder assessments, execution activities)**
    - **Developing a Branch-wide Network to enhance internal communications, provide unified external communications, and satisfy other vital communications objectives**
    - **Coordinating with other strategic communications initiatives within OIA, TSA, and DHS, to maintain cohesive and united messaging**
- Draft informational content for press releases, public affairs guidance, and website posting and routinely review the information for irrelevant or outdated content.
- Draft and upon government approval, issue informational material on the Secure Flight Program to internal and external stakeholders (aircraft operators, travel agencies, trade associations, congress, GAO, the press etc.). Informational material will be in various forms including, but not limited to meeting content, newsletters, presentations, toolkits, job aids, correspondence, and letters.
- Support Secure Flight Program senior leadership by drafting presentations, talking points, and briefings materials.
- Provide critical analysis of information to assist in the development of accurate Secure Flight Program communications products.
- Assist in building strong partnerships within Secure Flight and OIA to increase effectiveness and awareness of communications products and requirements.
- **Attend Secure Flight and OIA meetings and lead communications-specific support and tasks for regularly scheduled daily/monthly meetings that require internal and/or external messaging (e.g., system enhancements, process improvements, product changes)**
- Draft and upon government approval, update and distribute Communications Standard Operating Procedures (SOP).
- Provide support to coordinate, manage and execute all aspects of aviation industry conferences.
- Draft, coordinate and disseminate periodic Secure Flight Program Newsletters.
- Support Secure Flight Program visits, tours, and demonstrations.

- Review and provide Secure Flight comment and coordination on externally produced documents.
- Develop and maintain the Secure Flight portfolio of key messages, templates, and other vital communication tools that will be an accessible resource within Secure Flight and OIA
- Streamline and improve the iShare site. Includes archiving communication products on TSA's IShare site for easy identification and retrieval.
- Assist in drafting and coordination of responses to requests for information from Congress and TSA or DHS leadership.
- Assist DIA and other offices with communications support and review of products pertaining to the Secure Flight Program.
- Additional Stakeholder Communications as required.

3.3.2 Technical Writing and Document Management

- Provide quality assurance of program communication products which are produced under section 3.5 in this SOW.
- Maintain and update the Secure Flight Style Guide, the Secure Flight glossary, and the Secure
- Flight Acronym List.
- Support key document and vital records library semi-annual reviews and updates.

3.3.3 Training

- Conduct training needs assessments for various Secure Flight entities.
- Draft training plan and training materials for Vetting Dperations Division as outcome from the training needs assessments.
- Draft, maintain and refine New Hire Training course materials, transitioning appropriate modules to blended learning approach including a computer-based training.
- Deliver instructor-led courses.
- Draft and deliver system course materials for all Secure Flight System Releases and new operational technologies based on release schedule.
- Assist in analysis of new program initiatives to determine training requirements.
- Propose training delivery methods and program initiated course materials to support the rollout of new features, population and capabilities based on pilot and go-live dates.
- Propose, coordinate, and facilitate Domain and Initiative Awareness programs (In-the-Know) for Vetting Operations Division.
- Draft appropriate job aids to support external stakeholders.
- Support resource management and efficiency efforts by identifying and instituting standardized training processes and tools.
- Workforce Development/Employee Development:
- Establish a comprehensive OIA career progression strategy and plan that encompasses: position management, competency modeling, and career path development. Supporting activities include, but are not limited to:
- Reviewing existing cover sheets, position descriptions, and banding requirements.

- Interviewing workforce and stakeholders, to include conducting focus groups and workshops
- Mapping current state and developing the future state.
- Liaising with Human Capital and other key stakeholders
- Gathering behavioral data through various means
- Auditing work activities
- Creating and validating competency model
- Determining the proficiency level for each position
- Researching skills and professional experiences required or recommended for each position/level
- Identifying, defining, and validating career promotion and professional development paths
- Support personnel career development by identifying appropriate training and professional development opportunities in the areas of: training opportunity awareness, curriculum development, and supervisor support.
- Draft an employee development plan for Vetting Operations Division.
- Draft career-progression roadmaps for non-intelligence analysts.
- Draft a job rotation and Vetting Operations Division-level, cross-training program.
- Support Skills Gap Analysis for employees or team to identify competency (knowledge, skills, and abilities) gaps.
- Draft a training catalog that can be posted on IShare and maintained, available for staff to develop one-stop-shop to address performance gaps.
- Draft a database-training plan (e.g. Terrorist Identities Datamart Environment -TIDE, etc.) coordinated with other agencies and vendors.
- Draft communications on training offered by DHS/TSA/OIA and others.
- Draft performance-based process training guidance – repository of training opportunities based on performance feedback.
- Draft a "cohort" training approach that would bring supervisors from different branches together in collaborative sessions.
- Draft supervisor toolkits.

NOTE: Work within the Training area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.4 Business Architecture, Process, and Planning

The Business Architecture, Process and Planning (BAPP) functional area currently supports multiple disciplines such as: updating and maintaining current Secure Flight business process model flows and updating and maintaining current requirements in business requirements matrices and other requirement artifacts. BAPP is responsible for ensuring that all requirements are traced to system uses cases and must work closely with the Technology Solutions Division to ensure all requirements are properly implemented. The contractor will perform the following work:

3.4.1 Business Exploration

- Propose and/or draft new business processes that could streamline or support the Secure Flight business model.
- Assist in the translation of Secure Flight high-level strategic goals into business requirements.
- Support the coordination of business requirements and use cases with impacted stakeholders. Ensure deployed systems meet business requirements. Ensure User Acceptance Testing (UAT) and Validation adequately address business goals, objectives, and requirements.
- Draft concept definition papers and business cases as necessary.
- Support Secure Flight business analysts to identify and improve common business practices and ensure standardization across the Secure Flight Program and the Vetting Operations Division.
- Manage the updates and change processes related to the Secure Flight Concept of Dperations (ConOps) document in alignment with the Department of Homeland Security's Strategic Plan, establish Secure Flight Program external governance plans, related processes and documentation.
- Support business continuity planning to assist the Secure Flight program; including subject matter expertise in planning and designing business continuity planning for all of the business areas of the Secure Flight program.

3.4.2 Release Planning

- Support the capture, sponsorship, and prioritization of requirements and changes for future release iterations through management of the New Idea Capture process and the Business Change Board.
- Assist to ensure proper impact assessment for change requests.
- Maintain the Program roadmap and capability prioritization pipeline.
- Support with the Technology Solutions Division to determine Secure Flight release milestones.
- Support the development and management of each release plan.

3.4.3 Requirements Management

- Draft and, upon government approval, manage business-centric requirements deliverables within each release, including documentation and validation of requirements tracing.
- Draft Business Requirement Matrices, Problem Reports (PRs) for requirements, and other requirements management artifacts, as needed (e.g. Business Architecture Document and Business Requirement Documents).
- Support business validation for tracing:
    - Business requirements to Standard Operating Procedures (SOPs)
    - Business requirements to system use cases.
    - System use cases to test plans.
    - Test plans to test results.
    - Support and coordinate User Acceptance Testing (UAT) across the program.
- Log requirements and related artifacts into Secure Flight repository tools.

- Support implementation of business and operational requirements development and management processes.
- Establish mechanisms for business transition planning and management capability to ensure clear communication within the Secure Flight Program and with stakeholders. Coordinate efforts with organizational change management and ensure a smooth transition from the current state to the desired state.

3.4.4 Operational Partners Management

Support the management of relationship and coordination activities with Secure Flight operational partners, including:

- TSA Transportation Security Redress Branch (TSRB);
- TSA Office of Risk Based Security (ORBS);
- Customs and Boarder Projection (CBP); and o Department of Justice's (DOJ's) Terrorist Screening Center (TSC).
- Assist with the documentation of operational partner agreements including Memoranda of Understanding (MOUs), Inter- and Intra- Agency Agreements (IAAs), Inter- and Intra-Departmental Agreements (IDAs), Interface Control Documents (ICDs), Service Level Agreements (SLAs), and others as needed.

3.4.5 Secure Flight Reporting

The contractor shall assist with managing the Secure Flight Reporting mailbox, including:

- Analyzing reporting data requests and confirming requirements with stakeholders.
- Researching data to satisfy requests, using available analytic tools.
- **Coordinating with the customer and technical teams to update and enhance current analytic tools such as the Boarding Pass Printing Review (BPPR) and Passenger Record Locator (PRL) tools and further enrich Secure Flight data to design and develop new analytic tools to improve current and analytical reporting requirements generated by field operations, analyst, and senior leadership.**
- **Coordinating with the customer and technical teams to modify existing reports and develop new reporting products to account for Secure Flight improvements and new analytical reporting requirements generated by field operations, analyst, and senior leadership.**
- Coordinating with other teams such as Technology Support and Reporting, **Systems Development and Technology, Mission Architecture and Process Innovation, Privacy, and other business and technical organizations** to fulfill requests.
- Performing quality assurance on outgoing Secure Flight Reporting data and content.
- **Coordinating and participating in daily and semi-annual communications meetings with internal and external stakeholders with respect to product format, distribution, content, and operational value, as part of the certification process.**
- Performing ongoing stakeholder management in areas such as data quality and interpretation. **This includes coordinating and facilitating meetings to bring in the appropriate parties, especially for more complex requests.**
- Developing and maintaining Secure Flight Reporting SOPs.

- **Developing report specifications, reporting requirements, and other products and processes with respect to improving the overarching Secure Flight reporting concept of operations.**
- Collaborating with other BAPP team members to recommend and implement Business Change Requests (BCRs) resulting from Secure Flight Reporting work.

Recommending and implementing operational process improvements, as needed.
NOTE: Work within the entire Business Architecture, Process, and Planning area may require Top Secret (TS), Sensitive Compartmentalized Information clearance level for some personnel.

3.5 Technical Support and Reporting

The contractor will support the Technical Support and Reporting team by providing resources with the technical expertise necessary to provide support for the various Secure Flight subsystems. Knowledge of the specific Secure Flight subsystems will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Data management
- Report development using Oracle Business Intelligence Enterprise Edition (OBIEE)
- Data analysis
- Root-cause analysis

The contractor will provide an additional five (5) hours of additional of phone accessible on-call support per a seven (7) day week, through utilization of the aforementioned skills outside of core business hours and core business days (as defined in Section F.2).

- **Weekday Hours ranging from 1800 to 0800 (night/early morning hours)**
- **Weekend Hours – All Day Saturdays and Sundays**
- **Holidays – All Day**

In addition to utilizing the aforementioned skills during core business hours/days and for on-call support, the contractor will provide support to include, but not limited to:

- **Updating, maintaining, and distributing recurring reports to support field operations, analysts, and senior leadership**
- **Developing, creating, and distributing approximately 1,000+ ad-hoc reports per calendar year of varying complexity in multiple file formats tailored for the end-user to provide time-sensitive, critical requirements analytics as high priority requests**
- **Dperating and maintaining multiple analytical tools such as DBIEE and customized data models to support field operations, analysts, and senior leadership**
- **Providing analytical support through compilation of data, analysis of information, and data aggregation via various file formatting (i.e. Microsoft Excel) for end-user consumption in support of decision making**
- **Providing overarching technical support with respect to the reporting systems and reporting products**

3.6 Performance Engineering

The contractor will support the Performance Engineering team by providing resources with the technical expertise necessary to perform sophisticated data analysis and modeling. Knowledge of specific Secure Flight data will be gained via experience on the team, but the contractor will provide resources with the following types of technical skills when requested:

- Statistical data analysis
- Data extraction and manipulation (requires extensive SQL and some programming knowledge)
- Ability to convey complex information to non-technical decision makers (data visualization)
- Mathematical modeling for impact and predictive analysis
- Ability to devise processes to evaluate a closed source system

4. Project Management & Reporting and Requirements

The contractor shall perform project management services and resources required for performance under this SOW. The contractor shall comply with existing OIA and/or program- specific Configuration Management processes and procedures for hardware, software, and documentation. **The contractor shall coordinate and facilitate integration of all activities performed by the contract teams to provide transparent value to the Government, as described in the sections (3.1 and 3.6). The contractor shall work with the Government (CO, COR, Functional Leads, etc.) to oversee and optimize available resources.** Specific requirements include but are not limited to:

- Contractor Work Breakdown Structure (CWBS)
- Cost, Schedule, Forecast and Performance Reporting
- Ad Hoc Reports

The contractor shall provide project management data within the monthly report, as identified in section 4.2 below.

4.1 Work Breakdown Structure

The contractor shall provide a resource-loaded contractor work breakdown structure (CWBS), outlining the proposed activities, resources and costs to complete the requirements of this SOW. This CWBS shall align seamlessly into, and reflect the respective work outlined in the Government- provided Integrated Master Schedule (IMS).

The draft resource-loaded CWBS shall be provided to the Government for approval within 10 working days of the start of this Task Order Period of Performance. The CWBS will list the work activities, duration of each task/activity, resources required, deliverables, and cost for each work activity to be performed. This shall be the baseline CWBS, against which progress will be measured. The CO and Task Order COR. must approve any deviation from this baseline. The contractor shall report based upon a resource-loaded CWBS for schedule and requirements tracking that is proposed by the contractor and approved by the government.

4.2 Monthly Report

The contractor shall provide a monthly report outlining the contractor's cost, schedule and performance for the project by Task Order.

The contractor shall provide contractor performance reports that show the status of the contractor's production and performance assessment against the expected performance goals. Reports should show the following at a minimum:

- Reporting period
- Progress/Status
- Current month's activities (broken out to tasks performed for each effort/activity with resource assigned)
- Percentage of completion
- Forecast of next month's activities
- Issues encountered and any corrective actions during the reporting period
- Funding to date
- Cumulative dollar and percentage of funds expended
- Total funds remaining
- Projected spending for next month
- Total projected Task Order costs
- Funding shortfall date (if applicable)
- Hours expended per resource

A draft monthly reporting format will be presented to the government for approval within fourteen (14) calendar days of the start of the Period of Performance of this Task Order. The monthly report shall be submitted to the COR at least three (3) business days prior to the Program Management Review (PMR) meeting.

4.3 Ad Hoc Reports

An Ad Hoc report is a report requested by the Program Business Functional Manager addressing an area of concern not listed as a formal deliverable.

4.4 Travel

The contractor will be reimbursed for reasonable and actual costs for transportation, lodging, and meals and incidental expenses in accordance with Federal Travel Regulations (FTR). Travel performed for personal convenience or daily travel to and from work at the contractor's facility or local government facility (i.e., designated work site) shall not be reimbursed. Prior to undertaking any travel other than local, the contractor shall submit a request for specific approval to the COR, listing names of individuals traveling and destinations, dates, purpose and estimated cost of the trip. The contractor will use the Travel Authorization form for all travel conducted. All requests for travel must be pre-approved by the government business functional lead and the COR, and must contain the information required on the Travel Request Form (see TSA IShare), to include an estimated amount not to exceed expenses consistent with Joint Travel Regulations and GSA per diem schedules.

4.5 PMR Meeting

The contractor shall conduct Monthly Program Management Reviews to present to the government information on project status to include: Performance measurements, progress towards completion, associated risks, issues and cost. The information shall be provided with summary and appropriate

details of status and projected performance in the following areas: Functional performance and progress, project risks and mitigation progress, establish logical and realistic corrective action plan(s) to address identified issues, and establish priorities for execution based on the criticality of identified issue(s). Any issues identified during this review that need resolution shall be recorded and tracked by the contractor in an Action Item database. The status and disposition of all open action items shall be presented at the program review meeting, noting that disposition of each action item requires approval of the appropriate government representative - Project Manager (PM), Task Order COR, or CO. The contractor shall minimize resources and costs in connection with the monthly PMR meetings. The contractor shall conduct meetings before the fifteenth (15th) business day of the month, unless otherwise directed by the government.

5. Deliverables

The following table describes the Contract Data Requirements List (CDRLs) that are required for this SOW. The Contractor requires express written approval from the CO before executing any change to the scope, content, and/or delivery schedule of the described work products and tasks in this SOW.

Table 1: Contract Data Requirements List

CDRL #	Deliverable	Description	Frequency	Reference
001	User Acceptance Testing (UAT) Analysis	Plan User Acceptance Testing Efforts: Evaluate User Acceptance Testing Results, identify system enhancements and recommend changes to improve operating efficiencies	Based on each release (estimated Quarterly)	SOW Sections 3.1.1.1 and 3.4.3
002	Parallel Testing Guidance	Write testing guides and procedures for the parallel testing phase of implementation	Update as needed	SOW Section 3.2.1
003	Parallel Testing Analysis	Create parallel testing analysis and report	As specified by airline implementation plans	SOW Section 3.2.1
004	Cutover Strategy and Criteria Plan	Write and develop airline cutover strategy and monitor individual airline cutover schedule compliance	As needed, to align with implementation of new Airline Operators	SOW Section 3.2.1

005	Cutover Readiness Review	Summarize cutover readiness for each Airline Operator	Weekly	SOW Section 3.2.1
006	Airline Operator Test Reports	Detailed results of onboard testing for each Airline Operator	At the conclusion of each Airline Operator's onboarding	SOW Section 3.2.1
007	Operational Readiness Test Plan	Write testing guides and procedures for the operational readiness testing phase of implementation	Update as needed	SOW Section 3.2.1
008	Consolidated User Guide (CUG)	Enhance/modify the Consolidated User Guide (CUG)	Update as needed	SOW Section 3.2.1
009	Secure Flight Style Guide, Acronym List, and Glossary	Maintain the Secure Flight style manual (guide), acronym list, and glossary	Quarterly updates as needed. Final Assessment Due at end of TO	SOW Section 3.3.2
010	**Secure Flight Comprehensive Training and Change Management Plan**	**Maintain comprehensive Training and Change Management plans which outline objectives, needs, strategies, timelines and curriculum for Vetting Operations Division staff**	**Update as needed. Final Assessment Due at end of TD**	**SOW Section 3.3.1. and 3.3.3**
011	Training Materials	Create/maintain training material detailed in the Secure Flight training plan	As specified in the Secure Flight Training Plan	SOW Section 3.3.3
012	Workforce Development/ Employee Development	Create/maintain employee development initiatives as identified in the employee development plan	Quarterly Submission of artifacts created. Annual updates as needed	SOW Section 3.3.3
013	Secure Flight Business Architecture	Modifications and/or enhancements to Secure Flight business requirements and business process model/flows	Due per functionality/project implementation and release (estimated Quarterly) Ad Hoc Emergency Process Change Requests	SOW Section 3.4.3

014	Ad-hoc and recurring reports	Various reports to transmit Secure Flight data to stakeholders to inform decision-making	Create as needed	SOW Sections 3.2.3, 3.5, 3.6
015	Contractor Work Breakdown Structure (CWBS)	Resource-loaded schedule, including cost, performance, and requirements tracking that the Contractor proposes and is approved by the Government for each Task Order. The CWBS contains scheduled work products and related services for each mission application and align with the program's IMS (if provided)	10 Working Days after Task Order issued, updates as needed	SOW Section 4.1
016	Monthly Report	Cost, Schedule, and Performance Report	Draft: Within 14 calendar days of the start of the Period of Performance of each Task Order Monthly: no later than 10th Business day of	SOW Section 4.2
017	Program Management Reviews (PMRs)	Monthly meeting to discuss Schedule, Costs, Resources, Technical issues, problems and resolutions	No later than the 15th Business Day of each month	SOW Section 4.5
018	Final Report	Summarizes support activities, "start to completion schedules", deliverables and results achieved relative to the performance objectives of this SOW	Draft report 15 working days prior to conclusion of work. Final report 5 working days after receipt of comments	SOW Section 5
019	Firm Fixed Price Proposal & SOW	Detailed Scope of Work with tasks breakdown and deliverables identified	No later than 90 days before execution of exercising the Option Period	SOW Section B.2

The dates shown in the Deliverables Table are the required initial delivery date, which initiates the government acceptance timeline described below. All plans and documents are intended to provide continuity with previous work performed and to provide a comprehensive set of program management guidance and reporting as well as systems development and management documentation.

All deliverables, existing plans and documents shall be used in their current form where applicable and shall be updated as appropriate to accommodate deficiencies, program and development changes. Documents listed but not currently existing shall be created and delivered at the time specified in the frequency column above. The contractor shall prepare and maintain all documentation in accordance with an industry standard best practice for auditable, repeatable engineering process to assure the availability and accuracy of a comprehensive, complete, and current set of plans, reports, and documents.

The contractor shall use the TSA Systems Development Life Cycle Guidance Document, version 2.0, (or updated version) for updating of systems development documentation form and content.
The list of documents and their content and format may be refined and tailored by mutual agreement between the government and contractor to assure quality program management, systems development, and systems operation and management. The contractor shall also use the TSA Style Guide when preparing all deliverables. The Style Guide can be found on the TSA intranet at:

http://tsaweb.tsa.dot.gov/tsaweb/intraweb/assetlibrary/web_best_practices_and_style_guide.pdf

(END OF SECTIDN C)

SECTION D - PACKAGING AND MARKING

D.1 Markings

All deliverables submitted to the TO Contracting Officer or the TO Contracting Officer Representative (COR) shall be accompanied by a packing list or other suitable shipping documentation that shall clearly indicate the following:
(a) Contract number;
(b) Task order number;
(c) Name and address of the consignor;
(d) Name and address of the consignee;
(e) Government bill of lading number covering the shipment (if any); and
(f) Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).

(END OF SECTION D)

SECTION E - INSPECTION AND ACCEPTANCE

E.1 Inspection and Acceptance

All contract deliverables, including documents and system implementations, require approval and formal acceptance by the Task Order COR. The Government will have up to 10 business days after receipt of a deliverable to accept or reject any deliverable. If the Task Order COR rejects a deliverable, the Contractor will be provided specific written comments detailing the basis for the rejection and recommended corrective action. The Contractor shall have up to 10 calendar days to address all specific written comments by either incorporating the requested Government changes or providing an explanation of why the Government-requested changes are not being incorporated. The Government will have an additional five (5) calendar days to review and provide a final decision regarding acceptance or rejection of the deliverable.

E.2 Scope of Inspection

Documents submitted by the Contractor shall be professional in content and presentation according to commonly accepted standards of writing and editing in the subject field. The Contractor shall provide electronic copies to the Government Program Manager, Task Order COR, Contracting Officer and any other specified Government representatives as directed by the Government when due. All documents shall be delivered in Microsoft Office format (including Word, Excel, PowerPoint, Access, Visio, and Project) or other formats accepted by the government by direction of the Task Order COR. Previously released documentation will be delivered in current format unless mutually agreed otherwise.

E.3 Basis of Acceptance

Final CDRL deliveries shall be accompanied with a letter of delivery and Government acceptance to be signed by the Task Order COR and Project Manager (PM).

E.4 Review of Deliverables

At any point in the process of the review of deliverables, the deliverable is considered accepted if the Government provides written acceptance or does not provide comments and/or change requests within fifteen (15) business days of the receipt of the deliverable.

E.5 Final Deliverables

The contractor shall provide two (2) Compact Disk- Read Only Memory (CD-ROM) copies of the set of all final documents at the end of each Task Order. All documents shall be delivered in a format mutually agreed to between the contractor and the government. Previously released documentation will be delivered in current format unless mutually agreed otherwise. CDRL content may be combined into one delivered document with notification.

(End of Section E)

SECTION F- PERFORMANCE

F.1 PERIOD OF PERFORMANCE

The period of performance for this task order will be for a base period of twelve (12) months from award date with two (2) 12 month option periods The period of performance will start upon all contractor personnel's completion of TSA's personnel security process and deemed suitable/eligible to start work.

F.2 PLACE OF PERFORMANCE

Contractor's personnel will work full-time during core hours (0800-1800) at TSA Annapolis Junction location. Frequent visits to TSA Headquarters location may be necessary in some circumstances and will be coordinated and approved by the COR and the contractor Program Manager. The contractor is expected to provide on-site support during this timeframe on an 8-hour per day, 5-day a week basis.

U.S. Department of Homeland Security
Transportation Security Administration
132 National Business Parkway
Annapolis Junction, MD 20701

F.3 GOVERNMENT FURNISHED FACILITIES

The Government identifies the following GFE and GFI for this effort:

- Use of Government-provided facilities for contractor office space;
- Computer-hosting facilities with appropriate power, space and environment;
- Operating environments to include a workstation;
- Documentation required for facility and system accreditation;
- OIA On/Off-boarding procedures and;
- Access to TSA's Online Learning Center (OLC) – TSA's automated training system used to meet the mandated privacy and security training requirements.
- Necessary access to the TSA Intranet (internal website) and related software tools
- Access to copier and duplicating equipment

F.4 TRAVEL REQUIREMENTS

Long distance Travel is required in support of this Task Order. The Government will reimburse travel in accordance with the Federal Travel Regulations. All travel must be pre-approved by the COR.
Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed.

(END OF SECTION F)

SECTION G- CONTRACT ADMINISTRATION DATA

G.1. CONTRACTING OFFICER (CO)

The Contracting Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue orders, obligate funds and authorize the expenditure of funds, and notwithstanding any term contained elsewhere in this contract, such authority remains vested solely in the Contracting Officer. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) In the event, the Contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:
NAME: Gloria Uria
PHONE NUMBER: 571-227-2429
EMAIL: Gloria.Uria@tsa.dhs.gov

G.2. CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COR) AND TECHNICAL MONITORS

1. The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

2. The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

TSA CDR:
NAME: Anthony Pinto
PHONE NUMBER: 240-568-5307
EMAIL: Anthony.Pinto@tsa.dhs.gov

3. The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

4. The responsibilities and limitations of the COR are as follows:

- The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
- The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
- The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
- The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
- The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
- The COR is not authorized to direct the Contractor on how to perform the work.
- The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
- The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

5. The responsibilities and limitations of the TM are as follows:

- Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.
- Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
- Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
- Informing the COR if the Contractor is not meeting performance, cost, and schedule milestones.
- Performing technical reviews of the Contractor's proposals as directed by the COR.
- Performing acceptance of the Contractor's deliverables as directed by the COR.
- Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

G.3 SUBMISSION OF INVOICES

(a) Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of

contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

(b) Invoice Submission Method: Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:
1) Facsimile number is: 757-413-7314

The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (e) of this clause.

2) U.S. Mail:
United States Coast Guard Finance Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake, VA 23327-4111

3) Email Invoices:
FIN-SMB-TSAInvoices@uscg.mil or
www.fincen.uscg.mil

(c) Invoice Process: Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Technical Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

(d) Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

(1) Via the internet: https://www.fincen.uscg.mil
Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

(2) Via the Payment Inquiry Form: https://www.fincen.uscg.mil/secure/payment.htm

(e) Invoice Elements: Invoices will automatically be rejected if the information required in subparagraph (a) (2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and DUNS number are not included in the invoice. All invoices must be clearly correlate invoiced amounts to the corresponding contract line item number and funding citation.

(f) Supplemental Invoice Documentation: Contractors shall submit all supplemental invoice documentation (e.g. copies of certified time sheets (as applicable), subcontractor invoices, receipts, signed receiving reports, travel vouchers, etc) necessary to approve an invoice along with the original invoice. The Contractor invoice shall contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Invoice charges shall be billed per appropriate Contract Line item Number (CLIN), period of performance and obligated funding. Unless otherwise authorized by fiscal law, funding from one CLIN may not be utilized to offset charges on another CLIN, specifically if it is different accounting and appropriation data. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Technical Representative.

(h) Frequency of Invoice Submission: Invoices may be submitted on a bi-weekly or monthly basis. Once the invoicing method has been chosen, this method shall be the frequency of invoicing for the life of the Task Order.

(END OF SECTION G)

SECTION H- SPECIAL REQUIREMENTS

H.1 DISCLOSURE OF INFORMATION

Information furnished by the Contractor under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personally-identifiable information must be clearly marked.
Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the requirements of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.
In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and information and must ensure that all work performed by its Subcontractor(s) shall be under the supervision of the Contractor or the Contractor's employees.

H.2 PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION

Publicity releases in connection with this contract shall not be made by the Contractor unless prior written approval has been received from the Contracting Officer.
The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. Two copies of any material proposed to be published or distributed shall be submitted to the Contracting Officer.
A minimum of five full business days' notice is required for requests made in accordance with this provision.

H.3 CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT, AND SUPPLIES

If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property. The Contractor is responsible for maintaining all assigned space(s) in a clean and orderly fashion during the course of this contract. All telephones are for conducting official Government business only.

H.4 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.

(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.5 INTERRELATIONSHIP OF ASSOCIATE CONTRACTORS

The T5A may enter into contractual agreements with other Contractors (i.e., —Associate Contractors) in order to fulfill requirements separate from the work to be performed under this contract, yet having a relationship to performance under this contract. It is expected that contractors working under TSA contracts will have to work together under certain conditions in order to achieve a common solution for T5A. The Contractor may be required to coordinate with other such Contractor(s) through the cognizant Contracting Officer (CO) and/or designated representative in providing suitable, non-conflicting

technical and/or management interface and in avoidance of duplication of effort. Information on deliverables provided under separate contracts may, at the discretion of the TSA and/or other Government agencies, be provided to such other Contractor(s) for the purpose of such work.
Where the Contractor and an associate Contractor fail to agree upon action to be taken in connection with their respective responsibilities, each Contractor shall promptly bring the matters to the attention of the cognizant CO and furnish the Contractor's recommendations for a solution. The Contractor shall not be relieved of its obligations to make timely deliveries or be entitled to any other adjustment because of failure of the Contractor and its associate to promptly refer matters to the CO or because of failure to implement CO directions.
Where the Contractor and Associate Contractors are required to collaborate to deliver a service; the Government will designate, in writing and prior to the definition of the task, to both Contractors, a —lead Contractor for the project. In these cases the Associate Contractors shall also be contractually required to coordinate and collaborate with the Contractor. TSA will facilitate the mutual execution of Non-Disclosure Agreements.
Compliance with this Special Contract Requirement is included in the contract price and shall not be a basis for equitable adjustment.

H.6 NON-PERSONAL SERVICES

—Personal services are those in which contractor personnel would appear to be, in effect, Government employees via the direct supervision and oversight by Government employees. No personal services shall be performed under this contract. No Contractor employee will be directly supervised by a Government employee. All individual Contractor employee assignments, and daily work direction, shall be given by the applicable employee supervisor of the Contractor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.
The Contractor shall not perform any inherently governmental actions as defined by FAR 7.500. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government Contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change any contract and that if the other Contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.
The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this clause. Nothing in this special contract requirement shall limit the Government's rights in any way under any other term of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this special contract requirement shall be included in all subcontracts at any tier.

H.7 CONTRACTOR RESPONSIBILITIES

The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.

The Government shall not be liable for any injury to the Contractor's personnel or damage to the Contractor's property unless such injury or damage is due to negligence on the part of the Government and is recoverable under the Federal Torts Claims Act, or pursuant to another Federal statutory authority.
A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition.
The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall not:
Discuss with unauthorized persons any information obtained in the performance of work under this contract. Conduct business not directly related to this contract on Government premises.
Use computer systems and/or other Government facilities for company or personal business other than work related; or
Recruit on Government premises or otherwise act to disrupt official Government business.

H.8 QUALIFICATIONS OF EMPLOYEES

The Contracting Officer may require dismissal from work under this contract and/or removal of access to government facilities, property, information and/or information systems of those employees which the Contracting Officer deems incompetent, careless, insubordinate, unsuitable or otherwise objectionable, or whose continued employment the Contracting Officer deems contrary to the public interest or inconsistent with the best interest of national security.

H.9 NON-DISCLOSURE AGREEMENTS

Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive But Unclassified, Government procurement sensitive information, and/or other sensitive information, or proprietary business information from other Contractors (e.g., cost data, plans, and strategies). The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

H.10 OBSERVANCE OF LEGAL HOLIDAYS

The Government observes the following holidays:

New Year's Day	*Martin Luther King Birthday*
President's Day	*Memorial Day*
Independence Day	*Labor Day, Columbus Day*
Veteran's Day	*Thanksgiving Day*
Christmas Day	*Inauguration Day (Washington, DC metropolitan area)*

In addition to the days designated as holidays, the Government observes also the following days:
Any other day designated by Federal Statute,
Any other day designated by Executive Order, and
Any other day designated by President's Proclamation.

Observance of such holidays by Government personnel shall not be a reason for the Contractor to request an extension of the period of performance, or entitlement of compensation except as set forth within the contract. In the event the Contractor's personnel work during the holiday, they may be reimbursed by the Contractor, however, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, other than their normal compensation for the time worked. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.

When the Government grants excused absence to its employees in a specific location, assigned Contractor personnel at that same location may also be dismissed. The Contractor agrees to continue to provide sufficient personnel to perform critical tasks already in operation or scheduled, and shall be guided by the instructions issued by the Contracting Officer or the Contracting Officer's Technical Representative.
In the event the Contractor's personnel work during the holiday or other excused absences, they may be compensated by the Contractor, however, no form of holiday or other premium compensation will be considered either as a direct or indirect cost, other than their normal compensation for the time worked. For cost reimbursable and time and material (T&M) contracts, the government will only consider as direct and/or indirect costs those efforts actually performed during the holiday or excused absences in the event contractor personnel are not dismissed. This provision does not preclude reimbursement for authorized overtime work if applicable to this contract.
Otherwise, the management responsibility for contractor functions approved by the Contracting Officer for offsite work, in the event of inaccessibility of federal workplaces are the sole responsibility of the contractor. The contractor may propose telework or other solutions when critical work is required, however, the Contractor is solely responsible for any cost differential in performance, all liabilities that may be due to performance at an alternate location and all resources necessary to complete such performance.
In the event of an actual emergency, the Contracting Officer may direct the contractor to change work hours or locations or institute tele-work, utilize personal protective equipment or other mandated items.

H.11 ADVERTISING OF AWARD

The contractor shall not refer to contract awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

H.12 MAJOR BREACH OF SAFETY OR SECURITY

(a) Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Safety is essential to TSA and compliance with safety standards and practices is a material part of this contract. A major breach of safety may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of safety must be related directly to the work on the agreement. A major breach of safety is an act or omission of the Contractor that consists of an accident, incident, or exposure resulting in a fatality, serious injury, or mission failure; or in damage to equipment or property equal to or greater than $1 million; or in any "willful" or "repeat" violation cited by the Occupational Safety and Health Administration (OSHA) or by a state agency operating under an OSHA approved plan.

(b) Security is the condition of safeguarding against espionage, sabotage, crime (including computer crime), or attack. A major breach of security may constitute a breach of contract that entitles the Government to exercise any of its rights and remedies applicable to material parts of this agreement, including termination for default. A major breach of security may occur on or off Government installations, but must be related directly to the work on the agreement. A major breach of security is an act or omission by the Contractor that results in compromise of classified information or sensitive security information or sensitive but unclassified information, including contractor proprietary information, illegal technology transfer, workplace violence resulting in criminal conviction, sabotage, compromise or denial of information technology services, equipment or property damage from vandalism greater than $250,000, or theft greater than $250,000.

NOTE: Breach af Security far the purpases af this definition should not be confused with breach of security in screening operations.

(c) In the event of a major breach of safety or security, the Contractor shall report the breach to the Contracting Officer. If directed by the Contracting Officer, the Contractor shall conduct its own investigation and report the results to the Government. The Contractor shall cooperate with the Government investigation, if conducted.

H.13 CONTRACTOR STAFF TRAINING

The contractor shall provide fully trained and experienced personnel. Training of contractor personnel shall be performed by the contractor at its expense, except as directed by the Government through written authorization by the Contracting Officer to meet special requirements peculiar to the contract. Training includes attendance at seminars, symposia or user group conferences. Training will not be authorized for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer languages and computer operating systems that are available on the commercial market or required by a contract. This includes training to obtain or increase proficiency in word processing, spreadsheets, presentations, and electronic mail.

H.14 EMPLOYEE TERMINATION

The contractor shall notify the Contracting Officer immediately whenever an employee performing work under this contract who has been granted access to government information, information systems, property, or government facilities access terminates employment. The contractor shall be responsible for returning, or ensuring that employees return, all DHS/TSA -issued contractor/employee identification, all other TSA or DHS property, and any security access cards to Government offices issued by a landlord of commercial space.

H.15 STANDARDS OF CONDUCT AND RESTRICTIONS

The contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. Personnel performing work under this contract shall not:
Solicit new business while performing work under the contract;
Conduct business other than that which is covered by this contract during periods paid by the Government;

Conduct business not directly related to this contract on Government premises; Use Government computer systems or networks, and/or other Government facilities for company or personal business; Recruit on Government premises or otherwise act to disrupt official Government business.

H.16 ELECTRONIC AND INFORMATION TECHNOLOGY TO ACCOMMODATE USERS WITH DISABILITIES (SECTION 508 OF THE REHABILITATION ACT)

Section 508 of the Rehabilitation Act prohibits federal agencies from procuring, developing, maintaining, or using electronic and information technology (EIT) that is inaccessible to people with disabilities. The applicable standards in Section 508 of the Rehabilitation Act, as amended, shall apply to this contract and any items, or services covered by or provided in connection with this requirement. The Contractor shall provide items and services that comply with Section 508 requirements and the Electronic and Information Accessibility Standards at 36 CFR Part 1194.

H.17 WORKPLACE VIOLENCE PREVENTION

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be required to complete Workplace Violence Prevention training available through the TSA Online Learning Center. The course, entitled "Preventing Workplace Violence at TSA" shall be completed within 60 days of onboarding.

H.18 NOTIFICATION OF PERSONNEL CHANGES

The Contractor shall notify the Contracting Officer's Technical Representative (COR) in writing of any changes needed in building, information systems, or other information access requirements for its employees in order to meet contract requirements not later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to the COR: full name, social security number, effective date, and reason for change.

H.19 SUBSTITUTION OF KEY PERSONNEL

The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract's requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

(a) an explanation of the circumstances necessitating the substitution;

(b) a complete resume of the proposed substitute; and

(c) any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

H.20 CONTROLLED UNCLASSIFIED INFORMATION DATA PRIVACY AND PROTECTION

The Contractor shall be responsible for the security of: i) all data that is generated by the contractor on behalf of the Government ii) Government data transmitted by the contractor, and iii) Government 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 Government data, including but not limited to Personal Identifiable Information (PII), Sensitive Security Information (SSI), and Sensitive But Unclassified (SBU), and/or Critical Infrastructure Information (CII), shall be protected according to Department of Homeland Security information security policies and mandates.

At the expiration of the contract, the contractor shall return all Government information and IT resources provided to the contractor during the contract.

The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow all applicable DHS Component Agency's requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI, Informational Security and Privacy training, if required by the DHS Component Agency

The Contractor, and those operating on its behalf, shall adhere to the requirements of the non-disclosure agreement unless authorized in writing by the Contracting Officer.

The Government will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment as applicable. If encryption is required, the following methods are acceptable for encrypting sensitive information:

a. Products Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2.
b. National Security Agency (NSA) Type 2 or Type 1 encryption.
c. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

The contractor shall maintain data control according to the applicable DHS Component Agency's security level of the data. Data separation will 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 must comply with TSA MD 3700.4 if applicable. Users of Government 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 Government IT assets are expected to actively apply the practices specified in the TSA Information Technology Security Policy (ITSP) Handbook, Chapter 3, Section 6, Privacy and Acceptable Use, or similar DHS Component Agency's guidance or policy.

The contractor shall comply with the all data disposition requirements stated in the applicable DHS Component Agency's Information Security Policy. For all TSA orders the contractor shall comply with Information Security Policy Handbook Chapter 3, Section 17 Computer Data Storage Disposition, as well as TSA Management Directive 3700.4.

H.21 PERSONNEL ACCESS

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be subject to the security procedures set forth in this contract.

H.22 SUITABILITY DETERMINATION FOR CONTRACTOR EMPLOYEES

All contractor employees seeking to provide services to TSA under a TSA contract are subject to a suitability determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Office of Security, Personnel Security Division (PerSec), will allow a contractor employee to commence work on a TSA contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

A suitability determination involves the following three phases:

Phase 1: Enter On Duty Suitability Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination will include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final suitability determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed suitable to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Technical Representative (COTR) of the favorable determination. Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for final suitability adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

Phase 3: Final Suitability Adjudication: TSA PerSec will complete the final suitability determination after receipt, review, and adjudication of the completed OPM background investigation. The final suitability determination is an assessment made by TSA PerSec to determine whether there is reasonable

expectation that the continued employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final suitability determination will result in a notification to the COTR that the contractor employee has been deemed unsuitable for continued contract employment and that he/she shall be removed from the TSA contract.

H.23 SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE

(a) Definitions.

—Breach (may be used interchangeably with —Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

—Personally Identifiable Information (PII) as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII) as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

Driver's license number, passport number, or truncated SSN (such as last 4 digits)

Date of birth (month, day, and year)

Citizenship or immigration status

Financial information such as account numbers or Electronic Funds Transfer Information Medical Information

System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be —sensitive depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

Sensitive PII have higher impact ratings for purposes of privacy incident handling.

(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding its systems, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such

requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.
(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4
In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the contracting officer in coordination with CISO approves, written certification by the contractor that the following requirements are met:
(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;
(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements
(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
(6) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
(i) Authorized and official use;
(ii) Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;
(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.
(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.
The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.
(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one

hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

(f) Personally Identifiable Information Notification Requirement. The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security. Subject to Government analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

In the event that a PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

H.24 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 all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 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 non-disclosure 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 Technical Representative (COTR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

H.25 Contract Status Review

a. Background. Prompt, accurate data gathering, analysis and reporting enables both the Contractor and the Government to make sound decisions relating to performance under the contract. While the Contractor is solely responsible for performance, the Government wishes to be informed on all actions under the contract that affect compliance with contract cost, performance or schedule compliance.

b. Reporting Content. The Contractor shall provide information according to the slides included in the Contractor In-Process Status Review template that is attached to this contract. A matrix describing each slide and its reporting requirements follows:

Slide title	Deliverables
Requirement for contractor's	The contractor shall identify each major deliverable under the contract and identify the required delivery date and those activities that the

reporting	contractor has identified as critical to meet that delivery date

Slide title	Schedule
Requirement for contractor's reporting	The contractor shall report each item under the contract's schedule with the planned and actual dates for deliveries identified.

Slide title	Upcoming Events
Requirement for contractor's reporting	The contractor shall identify significant upcoming events as planned under or related to the contract that relate to contract performance.

Slide title	Human Resources/Staffing
Requirement for contractor's reporting	The contractor should include the elements as listed on the slide, with particular attention devoted to the extent to which the key personnel identified under the contract (by their positions) are actually filled and performing or what exact activities are underway to hire suitable candidates for performance.

Slide title	Risks
Requirement for contractor's reporting	The contractor shall report each risk area earlier identified (a red or yellow status item, anticipated cost overrun or late deliverable) and provide an assessment of the risks to the contract performance if the item is not capable of being remedied in time to attain the required contract performance.

Slide title	If Firm-Fixed Price
Requirement for contractor's reporting	The contractor should discuss delivery schedule compliance.

c. Reporting Method. The Contractor shall convene a meeting, located at the mutual convenience of the Contractor and Government that will include the Contractor's principal managers directing contract performance in which to explain the information presented in the attached slides. All persons identified as contractor "key personnel" in the attached contract will present the information contained in or related to their particular area of the contract status reporting template. The Government's Contracting Officer, Contracting Officer's Technical Representative, the Program Manager and other relevant Government personnel will attend. The Contractor should be able both to present information called for on the slide templates as well as questions from the Government related to them. During the course of the contract, this status reporting process is expected to generate action items for the contractor to address, and the status and progress of resolving each action item must be addressed at each meeting.

d. Reporting Frequency. The Contractor shall report the template information on a quarterly basis. The contractor shall deliver a copy of the final prepared charts for the required briefing to the COTR and Contracting Officer not later than two business days prior to the scheduled meeting.

e. Additional Requirements. The Government may, at its discretion, require additional items to be reported through the course of the contract and will provide additional instructions concerning such.

f. The effort required gathering data, report such, and conduct the required reporting process is included in the total price of this contract, and no activity related to these required status reports will be available for any further adjustment under the contract.

H.26 5200.225.001 Notice to Offerors/Contractors Concerning Trade Agreements terms applicability to the Transportation Security Administration (APR 2014)

With respect to the following Federal Acquisition Regulation (FAR) provisions and clauses listed directly below:

FAR 52.225-1 "Buy American Act—Supplies,"
FAR 52.225-2 "Buy American Act-Certificate,"
FAR 52.225-5 "Trade Agreements,"
FAR 52.225-6 "Trade Agreements Certificate,"
FAR 52.225-9 "Buy American Act—Construction Materials,"
FAR 52.225-10 "Notice of Buy American Act Requirement-Construction Materials,"
FAR 52.225-11 "Buy American Act—Construction Materials under Trade Agreements," and FAR 52.225-12, "Notice of Buy American Act Requirement—Construction Materials under Trade Agreements"

Offerors are hereby notified that the World Trade Organization Government Procurement Agreement presently makes the Transportation Security Administration (TSA) subject only to sources from within the following signatory countries: Canada, Chinese Taipei, Hong Kong, Israel, Liechtenstein, Norway, European Union, Iceland, and Singapore. Otherwise, the only other trade agreements that presently cover the TSA are the North American Free Trade Agreement and the U.S.-Chile Free Trade Agreement. The TSA cannot evaluate offers or award contracts to sources from countries not covered in these identified trade agreements or as specified herein. Offerors must analyze their intended proposals and provide information in response to the required provisions accordingly.

The European Union participation is as defined at
http://www.wto.org/english/thewto_e/countries_e/european_communities_e.htm

H.27 3052.245-70 GOVERNMENT PROPERTY REPORTS. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.
(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700–5, Contractor Report of Government Property.

H.28 TECHNICAL INSTRUCTION

(a) Performance of the work described herein may be subject to written or oral technical instructions issued by the Contracting Officer's Representative specified in Section 11.2 of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of specifications or technical portions of work description.
(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "Changes" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.
(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.
(d) Failure of the Contractor and the CO to agree on whether Government direction is technical direction or a Change within the purview of the "Changes" clause shall be a dispute concerning a question of fact within the meaning of the Clause of the General Provision entitled, "Disputes."
(e) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

H.29 5200.231.001 TRAVEL AND PER DIEM (APPLICABLE TO COST REIMBURSEMENT AND T&M TYPE CONTRACTS ONLY) (AUG 2013)

The Contractor shall be reimbursed for travel costs associated with this contract. The reimbursement for those costs shall be as follows:

- Travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.
- Per diem will be reimbursed, at actual costs, not to exceed, the per diem rates set forth in the Federal Travel Regulations prescribed by General Services Administration and when applicable, Standardized Regulations Section 925 – Maximum Travel Per Diem Allowances for Foreign Areas – prescribed by the Department of State.
- Travel of more than 10 hours, but less than 24 hours, when no lodging is required, per diem shall be one-half of the Meals and Incidental Expenses (M&IE) rate applicable to the locations of

temporary duty assignment. If more than one temporary duty point is involved, the allowance of one-half of the M&IE rate is prescribed for the location where the majority of the time is spent performing official business. The per diem allowance shall not be allowed when the period of official travel is 10 hours or less during the same calendar day.

- Airfare costs in excess of the lowest rate available, offered during normal business hours are not reimbursable.
- All reimbursable Contractor travel shall be authorized through the issuance of a task order executed by the Contracting Officer.

Local Travel Costs will not be reimbursed under the following circumstances:

- Travel at Government installations where Government transportation is available
- Travel performed for personal convenience/errands, including commuting to and from work; and
- Travel costs incurred in the replacement of personnel when such replacement is accomplished for the Contractor's or employee's convenience.

H. 30 5201.242.001 PERIOD DF PERFORMANCE FOR CDNTRACTS REQUIRING EMPLOYEE BACKGROUND CHECKS (AUG 2013)

The period of performance begins 60 days after contract award to allow for the Enter On Duty Suitability Determination. A contract modification shall be executed to revise the period of performance if the determination process is completed earlier.

The following restricts shall apply to this contract:

1. The Contractor will access classified material at the following TSA facilities: Annapolis Junction-132 National Business Parkway , Annapolis MD 20701 and TSA Headquarters -702 12th Street South, Arlington VA 22202

2. All contractor personnel assigned to this contract shall possess security clearances issued by the DSS commensurate with the level of required access to classified information that is directly in support of this contract. To perform on this contract, contractor personnel must possess a Secret security clearance, while others will be assigned to designated roles requiring access to Top Secret/Sensitive Compartmented Information (SCI). Those contractor personnel requiring access to SCI must be eligible under the provisions of Intelligence Community Directive (ICD) 704 without exception.

3. All contractor personnel requiring access to SCI as part of this contract effort must be approved and indoctrinated by DHS. Requests for Access will be submitted by the government project manager who can validate the justification for access. If approved for access, contractor personnel will receive an indoctrination briefing by TSA Special Security Office (SSO) security staff prior to being granted access to SCI. All personnel security reporting requirements of ICD 704 will

be made directly to the TSA SSO. Prior to leaving this contract, personnel will be scheduled for debriefing with the TSA SSO.

4. If required, the Contractor must store and safeguard SCI material in accordance with the applicable DCIDS or ICDs. Additionally, collaterally classified information (Confidential, Secret, and Top Secret) must be safeguarded, in accordance with DHS Instruction 121-01-011, "The DHS Administrative Security Program," and the Department of Defense (DOD) Manual 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM) for Safeguarding Classified Information." Additionally, the contractor must obtain prior written approval from the contracting officer or Contracting Officer Technical Representative (COTR) before executing NISPOM Chapter 5, Section 5-502, which authorizes the contractor to disclose classified information to cleared subcontractors. Further, NISPOM Chapter 5, Section 5-506, restricts the contractor from disclosing classified information received or generated under this TSA contract to any other Federal agency unless prior authorized is granted the Program office or contracting office. In accordance with the NISPOM, Chapter 5, Section 5-509, the contractor shall not disclose classified information to another contractor except to support a contract, subcontract or other TSA purpose.

5. Visits by contractor employees will only be certified by DHS when such visits are conducted as part of the contract effort.

6. SCI will not be released to contractor employees without specific approval of the originator of the material as outlined in governing directives and based on prior DHS approval and certification of their need-to-know. Inquiries pertaining to classification guidance and safeguarding procedures for SCI generated under this contract will be directed to the responsible Special Security Officer (SSO).

7. SCI provided in support of this contract remains the property of DHS or its component agency originator. Upon completion or cancellation of the contract, SCI materials will be returned to the direct custody of the responsible SSO, or destroyed in accordance with instructions outlined by the Contracting Officer.

(END OF SECTION H)

SECTION I- ADDITIONAL CLAUSES

The terms and conditions of the DHS TABSS Schedule shall govern with the following FAR and HSAR clauses that are either incorporated by reference or provided in full text herein. The complete text can be found at http://farsite.hill.af.mil/farsite_alt.html and click on current FAR and HSAR then select the appropriate clause.

I.1 52.204-1 APPROVAL OF CONTRACT (DEC 1989)

This contract is subject to the written approval of the Contracting Officer and shall not be binding until so approved.
(End of clause)

I.2 52.204-2 SECURITY REQUIREMENTS (AUG 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."
(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

I.3 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in section 31.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Department of Homeland Security
Transportation Security Administration
Office of Acquisition TSA-25
Attn: Gloria Uria
601 South 12th Street Arlington, VA 20598-6025

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(END OF SECTION I)

SECTION J- ATTACHMENTS

J-1	Non- Disclosure Agreement (to be executed on date of award)
J-2	SSI Cover Sheet
J-3	DD 254

(END OF SECTION J)

End of Task Order

Section H- Special Requirements

H.5200.252.001 "Order of Precedence in Security Related Terms" (MAR 2015).

In the case of any conflict between the Department of Homeland Security requirements for security in the following terms: (HSAR 3052.204-70, "Security Requirements for Unclassified Information Technology Resources" (JUN 2006), "Safeguarding of Sensitive Information" (MAR 2015), and "Information Technology Security and Privacy Training" (MAR 2015)) and any other term or clause in this contract, the aforementioned Department of Homeland Security terms shall take precedence. In case this contract otherwise includes HSAR 3052.204-70, "Security Requirements for Unclassified Information Technology Resources" (JUN 2006), the term "Safeguarding of Sensitive Information" (MAR 2015) takes precedence over HSAR 3052.204-70.

(End of Special Contract Requirement)

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
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

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

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

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of

compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Hondbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorizotion Process Guide* including templates.

(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 *NI5T Special Publicotion 800-53 5ecurity and Privacy Controls for Federal Informatian Systems and Organizatians*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) 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 Informotion 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, and

(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) *Additionol PII ond/or SPII Notificotion 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 Privocy Incident Hondling Guidonce*. 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 Dfficer 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.*

(End of clause)

Information Technology Security and Privacy Training (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) *Security Training Requirements.*

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

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting,

storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

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

(End of clause)

Section I- Contract Clauses

H5AR 3052.204-71 CONTRACTOR EMPLOYEE ACCE5S (5EP 2012)

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, 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)

ALTERNATE I (SEP 2012)

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

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

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

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

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

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

(2) The waiver must be in the best interest of the Government.

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

(End of clause)