SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER: 2415205CT2530

PAGE 1 OF 5

2. CONTRACT NO.: HSHQDC-13-D-E2090

3. AWARD/EFFECTIVE DATE: 09/01/2015

4. ORDER NUMBER: HSTS04-15-J-CT2530

5. SOLICITATION NUMBER:

6. SOLICITATION ISSUE DATE:

7. FOR SOLICITATION INFORMATION CALL: ▶

a. NAME: Steven Santos

b. TELEPHONE NUMBER *(No collect calls)*: 571227 (b)(6)

8. OFFER DUE DATE/LOCAL TIME:

9. ISSUED BY CODE 20

OFFICE OF ACQUISITION
701 S 12TH STREET
Arlington VA 20598

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 541519

SIZE STANDARD: $27.5

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE

12. DISCOUNT TERMS: Net 30

☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION ☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE ACQ04

SECURITY TECHNOLOGY
701 S 12TH STREET
Attn: STEVEN SANTOS
Arlington VA 20598

16. ADMINISTERED BY CODE 20

OFFICE OF ACQUISITION
701 S 12TH STREET
Arlington VA 20598

17a. CONTRACTOR/OFFEROR CODE 079428492 FACILITY CODE

Computer Sciences Corporation
Attn: David Zolet
1200 S Hayes St
Arlington VA 222025005

TELEPHONE NO. 703-6413735

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE TSA1

US Coast Guard Financial Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake VA 23327-4111

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Tax ID Number: 95-2043126 DUNS Number: 079428492 Period of Performance: 09/01/2015 to 08/31/2016				
00001	Security Management Accounting Info: 5AV145A000D2015SWE030CE014623006200622CTO-62020000 00000000-251B-TSA DIRECT-DEF. TASK-D Continued ...				341,694.00

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA: See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $3,507,493.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 2 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT: ______ OFFER DATED ______. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR: Melissa S Greene

30b. NAME AND TITLE OF SIGNER (Type or print): Melissa S. Greene, Contracts Mgr

30c. DATE SIGNED: 8-25-15

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER): Steven D. Santos

31b. NAME OF CONTRACTING OFFICER (Type or print): Steven Santos

31c. DATE SIGNED: 8/26/2015

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

Working Copy

SECTION II – STATEMENT OF WORK

Security Technology Integration Program (STIP)

Contents

1. Background Information 3

2. Technical and Operational Overview 3

2.1 STIP Applications and Capabilities 3

2.1.1 STIP Enterprise Manager (EM) 3

2.1.2 Service Management Application (SMA) 4

2.1.3 Government Property Management (GPM) System 4

2.1.4 TSE User Management (TUM) 4

2.1.5 Threat Image Projection (TIP) 4

2.1.6 STIP Technology Reports 4

2.2 STIP STAKEHOLDERS AND USERS 4

2.3 APPLICABLE DOCUMENTS 6

2.4 STIP O&M SUPPORT TASKS 7

2.5 STIP APPLICATION SUITE (STIPAS) COMPONENTS 7

2.6 APPLICABLE DOCUMENTS 8

3 Objective 9

4 Scope of Work 9

5 Task 1: STIP Help Desk Support 10

5.1 STIP Network Monitoring & Health Support 10

5.2 Tier I and II Troubleshooting Support 11

5.2.1 Tier I Troubleshooting Support 11

5.2.2 Tier II Troubleshooting Support 12

5.2.3 Ticket Escalation Process 12

5.3 Application Build Support) 13

5.4 Testing and Deployment Support 13

5.5 Infrastructure Gap Remediation (IGR) 15

5.6 Operations and Maintenance Dispatch Support 15

6 Task 2 – TSIF Support 15

7 Task 6 – Engineering Services 17

8 Task 7 – Program Management 17

8.1 PROGRAM Status Report (Del 182) 17

8.2 Meetings and Reviews (Del 183) 18

8.3 Deliverable Schedule 18

8.4 Post Award Conference 18

9 Miscellaneous 19

10 Transition Activities 19

11 Place of Performance 20
12 Travel and ODCs 20
13 ITIP Bridge Task Order Performance Work Statement 20

1. Background Information

The Security Technology Integration Program (STIP) is an agency wide information technology program within the TSA Office of Security Capabilities (OSC) which enables TSA to move their established airport security system to the next generation of capability by connecting myriad Transportation Security Equipment (TSE) to one network. STIP establishes a centralized enterprise data management system, the Enterprise Manager (EM), that facilitates the exchange of information between TSE located at the nation's airports and the people who use and maintain them. STIP supports new innovative approaches to exchanging information and servicing equipment, assisting managers in more effectively administering TSE, deploying personnel, and adapting to changing security needs.

STIP is structured into multiple, distinct work streams that will implement the full STIP capability over a period of time. The timeline for full realization of the STIP capability is dependent on implementation of enhanced TSA business processes to leverage the full STIP capability.

2. Technical and Operational Overview

The STIP Application Suite (STIP AS) comprises a number of separate applications and interfaces with many different systems within TSA. These include the STIP Enterprise Manager (EM), Threat Image Protection (TIP) applications, TSE User Management (TUM), and the government Property Management (GPM) Database.

STIP connects with the remote TSE by using a STIP Agent that resides on each individual TSE. The basis for the communication between the Agent and the STIP EM is defined in the STIP Interface Requirements Document (IRD). The IRD has been developed to identify the functional design characteristics for the data transfer between the TSE and the STIP EM.

The STIP also interfaces with Secure Flight in support of the Credential Authentication Technology (CAT) Networked Solution as well as the Service Management Application (SMA) to assist in automating OSC's configuration management processes. In the future, STIP will also interface with the Electronic Performance Management Platform (ePMP) to alleviate the burden of manual data collection currently experienced by the Office of Security Operations (OSO).

2.1 STIP Applications and Capabilities

2.1.1 STIP Enterprise Manager (EM)

The STIP EM consists of the legacy system, STIP Legacy Axeda, which is currently being phased out, and the STIP Enterprise Mission Manager (STEMM), which is the new system, currently being phased in.

2.1.1.1 STIP Enterprise Mission Manager (STEMM)

STEMM connects the STIP servers and TSE via a standards-based, government-owned custom software solution. STEMM and associated functionality will replace the legacy system, increasing reliability and scalability to accommodate future needs.

2.1.1.2 STIP Legacy Axeda EM

Axeda is a Commercial-Off-The-Shelf (COTS) product that connects the STIP servers and the remote TSE. This is accomplished by using an Axeda Agent that resides on each individual TSE as well as a COTS Enterprise Management solution which is hosted on centralized STIP servers.

2.1.2 Service Management Application (SMA)

SMA is a system that interfaces with both the STIP EM and GPM to capture configuration change information on TSEs. TSA business efficiencies will be impaired if any piece of SMA connectivity is broken. The primary users of the SMA system will be the Integrated Logistics Support (ILS) Branch to track configuration changes on TSEs.

2.1.3 Government Property Management (GPM) System

GPM system is an asset management database that tracks asset information related to security equipment and serves as the system of record for OSC. The information is maintained in the system by ILS.

2.1.4 TSE User Management (TUM)

TUM is a user management database that tracks information related to security equipment user access. It is the system for TSA Globally Unique User Identification (GUUID). The information is maintained in the system by airport personnel with STIP Help Desk support.

2.1.5 Threat Image Projection (TIP)

TIP tests a Transportation Screening Officer's ability to detect known threats by X-ray. Potential threat images, including guns and explosives, are projected onto real X-ray images of carry-on bags and TSOs are scored on their ability to recognize and properly resolve these images. STIP has developed a suite of application to support the automated management of library images and analysis of TIP performance data.

2.1.6 STIP Technology Reports

STIP Technology Reports is the data analytics and reporting application within the STIP AS. These reports can be accessed through the OSC portal. Data from each report are pulled into graphics and tables to help analyze the information being collected.

2.2 STIP STAKEHOLDERS AND USERS

There are several user groups and stakeholders that will utilize STIP and its capabilities; these groups span multiple offices within and external to TSA. As new capabilities are identified and TSA's needs evolve, STIP will likely be relied on for capability enablement and enhancement.

STIP Capability	User Group
Security: Dynamic transfer of information between the enterprise and TSE.	• Transportation Security Officers (TSO) • STIP Help Desk Administrators
Configuration Management: Automatic upload of configuration updates and software on TSE, as well as capability to efficiently collect, track, and harmonize configuration settings on TSE.	• Configuration Managers (CM) • GPM Users • TIP Administrators • Original Equipment Manufacturers (OEM) • STIP Help Desk Administrators
Information Sharing and Enterprise Management: Automated data collection processes used to capture	• Reporting Users • STIP Help Desk Administrators

STIP Capability	User Group
and maintain operational data for TSE.	
Resource Management: Collection and maintenance of TSO performance data from TSE as well as user management capabilities.	• Reporting Users • TIP Administrators • TUM Administrators • STIP Help Desk Administrators
Remote Monitoring and Maintenance: Remote monitoring and maintaining of TSE health.	• Field Service Technicians (FST) • TSA Service Response Center (TSRC) • Reporting Users • STIP Help Desk Administrators

Table 1: STIP Users

STIP also has various TSA stakeholders that do not interact with the system directly but are involved in the planning and implementation of different programmatic aspects. Those stakeholders are aligned to STIP's core capabilities.

STIP Capability	Stakeholder Group
Security: Dynamic transfer of information between the enterprise and TSE.	• Office of Security Operations (OSO) • Office of Security Capabilities (OSC), including the Mission Analysis Division (MAD), the Passenger Screening Program (PSP), and the Electronic Baggage Screening Program (EBSP) • Office of Intelligence and Analysis (OIA) • Office of the Chief Risk Officer (OCRO) • Office of Information Technology (OIT)
Configuration Management: Automatic upload of configuration updates and software on TSE, as well as capability to efficiently collect, track, and harmonize configuration settings on TSE.	• OSO • OSC, including the Deployment and Logistics Division (DLD), PSP, EBSP • OEMs • OIT
Information Sharing and Enterprise Management: Automated data collection processes used to capture and maintain operational data for TSE.	• OSO • OSC, including DLD, PSP, EBSP • OIA • OIT
Resource Management: Collection and maintenance of TSO performance data from TSE as well as user management capabilities.	• Office of Training and Workforce Engagement (OTWE) • OSO • OSC • OIT
Remote Monitoring and Maintenance: Remote monitoring and maintaining of TSE health.	• OSC, including the Deployment Division, PSP, EBSP • OEMs • Maintenance Service Providers (MSP) • OIT

Table 2: STIP Stakeholders

2.3 APPLICABLE DOCUMENTS

The following government documents provide technical overview and guidance:

Document Name	Description
TSA Management Directive (MD) 1400.3	TSA MD No. 1400.3 - TSA Information Security Policy – March 15, 2008
Department of Homeland Security (DHS) 4300 A	DHS Sensitive Systems Handbook V11.0 – April 30, 2014
Federal Information Processing Standards (FIPS) 140-2	Security Requirements for Cryptographic Modules - December 3, 2002 (Change Notice 2)
OIT Release Change and Configuration Management (RCCM) Process	This document provides an overview of the Release Configuration Change Management (RCCM) process for TSA's Office of Information Technology (OIT) Customer Engagement & Development Division (CEDD). The purpose of the RCCM is to ensure service delivery is accomplished using high quality, repeatable and well documented processes. The following topics are covered in this document: - New, Major, Significant or Minor Applications Releases - Infrastructure Releases (OED or outside vendor initiated changes and patches) - Repair Operations Releases (data fix only, no code changes)

Table 3: Government Documents for Guidance

The following STIP documents are applicable to this Statement of Work (SOW):

Document Name	Description
STIP Concept of Operations (CONOPS), V2.0	The CONOPS documents the high level requirements of STIP, and describes the characteristics of the system from the users' perspective.
STIP Functional Requirements Document (FRD), V1.5	The FRD describes the features and functionality of the system.
Interface Requirements Document (IRD) 4.14	The IRD establishes, defines, and is the controlling interface and for documenting detailed interface design definition for the STIP program.
STIP AS System Design Document (SDD), V1.5 Rev K	The SDD defines the high level design for all components of STIP.
STIP Operation Requirements Document (ORD) v2	The ORD describes the high level operational requirements for the STIP system.
STIP CAT Data Management Console (CDMC) and Secure Data Monitor (SDM) Admin Manual	This STIP CDMC and SDM User Manual System Administrative Role are to help System Administrators to understand and maintain STIP CDMC and SDM.

Detailed Design Document (DDD) for the STIP Databases	This DDD establishes the design for the development of the STIP database instances.
STIP Requirements Validation Document (RVD) 2.9	The RVD establishes the requirements for the development of the software products for STIP.
STIP Secure Flight Interface Control Document (ICD)	This document establishes the functional and performance interface requirements between STIP and Secure Flight.
STIP ePMP Interface Control Document (ICD)	This document establishes the functional and performance interface requirements between STIP and ePMP.

Table 4: STIP Documents for Guidance

2.4 STIP O&M SUPPORT TASKS

This requirement is comprised of seven (7) core tasks that will be covered in more detail in subsequent sections.

1. STIP help desk support
2. STIP TSIF environment support
3. TSE and software deployment support
4. TSE connectivity and maintenance support
5. STIP network security support
6. STIP engineering support requests
7. Program management

2.5 STIP APPLICATION SUITE (STIPAS) COMPONENTS

This section provides an overview of the following STIPAS components:

STIPAS Component	Description
OSC Portal	The OSC Portal provides a single sign-on (SSO) solution for STIPAS users and provides links to the STIPAS applications. This STIPAS SSO solution does not integrate with TSA applications outside the STIPAS.
STIP Agent	The Axeda Service Link system is a COTS product. Its main purpose is to enable communication between the STIP central servers and the remote TSE. The Service Link system accomplishes this through the use of a software agent (the STIP Agent) residing on the TSE and a Service Link Enterprise Manager (Service Link EM) residing on the central STIPAS application servers. In addition to communication to the TSE, the Service Link EM also provides a browser-based interface for management of the TSE, data analysis and reporting.
STIP Enterprise Manager (STIP EM)	Custom extensions to Service Link EM allow OST users to centrally manage the TSE configuration parameters and TSE software versions on the TSE. The out-of-the-box Service Link EM application, the Cognos business

STIPAS Component	Description
	intelligence tool, and the STIP-specific customizations and extensions to the Service Link EM are collectively referred to as the STIP EM.
TIP Library Management (TLM)	Authorized STIP users may utilize the TLM application to manage the TIP images included in a specific TIP library version, or to create a new TIP image library version that can be assigned to TSE devices using the TIPCM application. The STIP user can view the image thumbnail or the full image, activate/inactivate the image, change the image's category, add image categories, and include or exclude the image in a specific library version.
STIP/Secure Flight Interface	The Secure Flight Interface with STIP is responsible for the transfer of information from Secure Flight to STIP.

Table 5: STIP Application Suite Components

2.6 APPLICABLE DOCUMENTS

The following government documents will provide background on the STIP system:

Document Name	Description
TSA MD 1400.3 Version 10.0	Transportation Security Administration (TSA) Management Directive No. 1400.3 - TSA Information Security Policy - May 20, 2013
DHS 4300 A	Department of Homeland Security Sensitive Systems Handbook V6.1.1 - May 14, 2008
FIPS 140-2	Security Requirements for Cryptographic Modules - December 3, 2002 (Change Notice 2)
TSA SDLC	Transportation Security Administration (TSA) Systems Development Lifecycle
EAS SQL Scripts Standards and Guidelines v3.0	Identifies standards and guidelines for SQL scripts.

Table 6: Applicable Government Documents

The following STIP documents are applicable to this SOW:

Document Name	Description
STIP Concept of Operations (CONOPS), V1.2	The CONOPS documents the high level requirements of STIP, and describes the characteristics of the system from the users' perspective.
STIP Functional Requirements Document (FRD), V1.4	The FRD describes the features and functionality of the system.
STIP Application Suite System Design Document (SDD), V1.5 Rev A	The SDD defines the high level design for all components of STIP.
STIP Operation Requirements Document (ORD) v1	The ORD describes the high level operational requirements for the STIP system.
OM 2011-007 Reset switch port to	Methodology RFC

Document Name	Description
clear MAC address violation for STIP	
RFC 2011-0030 Reset switch port to clear MAC address violation for STIP	Methodology RFC
RFC-2008-0264 Rev 2 Antivirus Port Opening	Methodology RFC
OM-2009-0663 Methodology	VLAN Configuration Consolidation
STIP TSE Connectivity SOP (draft CSC document)	Procedures and processes for connecting TSE to the TSANet.

Table 7: Applicable STIP Documents

3 Objective

The objective of this SOW is to provide support to the STIP program office in the seven core areas outlined above. Two of those areas, (5) Security Management Requirements, and (6) IT Engineering Services are leveraged from the ITIP Bridge Contract (HSTS03-15-J-CIO656).

This modification provides for tier pricing for the numbers of TSE supported, and aligns with the base IDIQ contract.

4 Scope of Work

The contractor shall provide the following tasks as stated in the table below. Each of these tasks and the deliverables associated with each task are defined in further detail in the subsequent sections. (Tier III support for all STIP applications is currently being provided by the STIP EM development contractor.) Please see Attachment 2 for a list of CLINs and descriptions.

Task Name	Task Description
STIP Help Desk Support	Actively monitor the connectivity and communications of STIP applications on the TSA network, including the health of the STIP EM, applications and connected TSEs. Provide Tier I support to users of the STIP Enterprise Manager and STIP Agent. Provide Tier II support to system owners, end users, and contractors of the STIP applications suite. Tier I and II support includes documenting, and reporting of issues and tickets from inception to closure.
TSIF Support	Provide engineering and hosting services to support two government-owned testing environments at a TSA facility in Arlington, VA (TSIF).
Deployment Support	Support for collection, coordination, and distribution of pertinent data is required for each new STIP deployment of EM applications, updates, new TSE deployments, and software deployments to TSE in the field. Liaise with appropriate stakeholders to gather and disseminate appropriate information related to a STIP deployment. Additionally, work with the deployment team to provide initial configuration settings and coordinate opening and verification of port connectivity.
TSE	The contractor shall monitor and ensure the TSANet connectivity of TSA's

Task Name	Task Description
Connectivity Maintenance Support	fleet of TSE. This task includes field dispatch.
STIP Security Management	Provide POAM and C&A support for the STIP program servers (not TSEs) per FISMA, DHS and TSA policies and procedures. As described in the ITIP Bridge (HSTS03-15-J-CIO656) Performance Work Statement.
IT STIP Engineering Services (ESRs)	As described in the ITIP Bridge (HSTS03-15-J-CIO656) Performance Work Statement.
Program Management Support	Provide Program Management Support for the STIP O&M Support

Figure 1: SOW Tasks

5 Task 1: STIP Help Desk Support

5.1 STIP Network Monitoring & Health Support

STIP Monitoring and Health Support

The contractor shall provide connectivity monitoring and troubleshooting of connected STIP enabled TSEs. These calls will originate from multiple sources. If it is found that a TSE goes offline for more than 24 hours, the contractor must begin the troubleshooting process, which includes calling the TSRC to see if there was a recent ticket opened for the machine, calling the airport to determine if the machine was intentionally taken offline, and working with the appropriate stakeholders to bring the machine back online. Once the machine is back online, the contractor will work with the appropriate Tier III support personnel to verify all of the expected data collected while the TSE was offline has been sent to the EM. Connectivity statistics will be tracked and provided to the government through the Program Status Report (as described in section 8.1).

Network Monitoring and Health Support

The contractor shall provide connectivity monitoring and troubleshooting of the STIP application suite as it resides on the TSA network (TSANet).

The contractor shall liaise with all applicable STIP stakeholders including the Office of Information Technology (OIT) Network Infrastructure contractor in order to address system health and connectivity issues that occur. The contractor shall be prepared to develop any applicable RFC in order to address and resolve a connectivity issue that arises. Connectivity statistics will be tracked and provided to the government through the Program Status Report (as described in section 8.1).

The contractor shall be responsible for preparation, submission and management of single occurrence and recurring RFCs. In the case of recurring RFCs the contractor shall be responsible for tracking the RFCs and re-submitting the RFCs to prevent a lapse in RFC coverage.

The contractor shall provide STIP network monitoring and health support Monday thru Friday from 8:00 AM to 5:00 PM (EST). The network monitoring shall include from the Wide Area Network (WAN) to the connected network switch The EM, which is supported by the Tier II STIP Operation Center, monitors from the connected network switch to the TSE.

5.2 Tier I and II Troubleshooting Support

TSA requires a Help Desk function to address user inquiries and encountered issues with STIP applications or network connectivity. The contractor shall document, report, resolve, or escalate all tickets as described in the Ticket Escalation Process 5.2.3.

The contractor shall provide a Help Desk function that with personnel who have functional knowledge about the STIP application suite and will be responsible for taking and troubleshooting telephone and email inquiries in support of the Enterprise Manager, GPM, STIP/Secure Flight Interface and STIP Agent applications.

5.2.1 Tier I Troubleshooting Support

The contractor shall serve as the single point of contact between all customers who open tickets for any of the STIP applications or systems and the other support contractors. The contractor shall have processes and procedures in place for keeping customers informed about the status of their issue, shall be in regular communications with the STIP PMO, OIT, and the STIP Development contractor support to coordinate any known connectivity outages, and maintain high customer satisfaction ratings.

The contractor shall understand issues related to the RMM and TFA, and know to escalate these issues to the appropriate service level for resolution. If further diagnosis is required, the contractor shall provide troubleshooting support to address STIP system issues, user additions or deletions, and problems with STIP applications or network connectivity. The contractor shall document, report, resolve, or escalate all tickets as described in the Ticket Escalation Process 5.2.3.

The contractor shall provide a service desk, leveraged from the ITIP Bridge Task Order, for troubleshooting telephone, email, and ticketing system issues in support of the Enterprise Manager, RMM, GPM, STIP/Secure Flight Interface and STIP Agent applications. The contractor shall provide basic help desk support 24x7x365. The contractor shall track trouble tickets in a consolidated database to closure and communicate ticket updates at regular intervals to STIP stakeholders.

For tickets associated with username additions or deletions, the contractor shall request the necessary permissions from TSA stakeholder groups and implement user additions or deletions from STIP applications. Should additional user access be needed from a system outside of the STIP application suite, the contractor shall coordinate the effort to obtain the access through the necessary stakeholders and the STIP system owners

The contractor shall support other maintenance tasks. The maintenance tasks consist of:

- Port resets;
- Troubleshooting connectivity issues, e.g., network;
- Work with maintenance service providers (MSPs) to troubleshoot maintenance issues, e.g., bad TSE network card;
- Work user IDs and password issues with Threat Image Projection (TIP) contractor as they arise;

- Establish and maintain user IDs and passwords for MSP, OEMs and TIP contractor;
- Create and maintain a database of the data capture sheets to facilitate troubleshooting.
- Other tasks similar to those above.
- The contractor shall support software updates. The software update tasks consist of:
- Support software updates pushed by the STIP EM to TSE
  - Application updates
  - Security patches
  - Software deployments
- Other software deployment tasks similar to those above.

The contractor shall coordinate updates with each airport and schedule an acceptable time (usually when checkpoints are closed).

5.2.2 Tier II Troubleshooting Support

The contractor shall be responsible for investigating and resolving all issues that do not require coding changes or database modifications.

The contractor shall have processes and procedures in place for keeping customers informed about the status of their issue, shall be in regular communications with the STIP PMO, OIT, and the STIP Development contractor support to coordinate any known connectivity outages, and maintain high customer satisfaction ratings. The contractor shall liaise with stakeholders related to assigned tickets in order to drive tickets to completion.

The contractor shall be responsible for investigating and resolving connectivity issues. The contractor shall notify the appropriate support teams and the issue will be tracked to closure.

The contractor shall provide support to aid in the diagnosis of complicated and technical STIP-related incidents.

The contractor shall provide Tier II STIP Operation Center support Monday thru Friday from 8:00 AM to 5:00 PM (EST).

5.2.3 Ticket Escalation Process

The contractor shall use the following process for escalating STIP Application tickets:

- If a ticket cannot be closed, the ticket shall be escalated to the next level of support.
- If no resolution is found the ticket will remain open and forwarded to the STIP Development support contractor.
- If no resolution is found in at the STIP Development contractor support, the ticket will remain open and the issue will be forwarded to the STIP program leadership. The STIP leadership is defined as the STIP Program Manager, STIP Deputy Program Manager and STIP Help Desk COTR.
- If a resolution is found at any stage in the process, but not implemented to resolve the issue, the ticket shall remain open in an "on hold" status.
- A ticket may only be closed when the issue is resolved or if deemed out of scope by STIP program leadership.

The contractor shall be responsible tracking the ticket to closure. As the owner of all STIP tickets, the contractor shall responsible for collecting updates from various fix agents and update the tickets, and report the ticket status. The contractor will serve as the single point of contact for all tickets.

5.3 Application Build Support

Please reference ITIP Bridge PWS, Section 3. TSA anticipates approximately eight (8) medium-sized releases and 52 incidents, inclusive of break/fix RFC implementations.

5.4 Testing and Deployment Support

The contractor shall provide support for pilot testing of STIP devices, including testing connectivity, and monitoring devices for connectivity issues. The government will provide airport network information prior to deployment in the form of a data capture sheet. The contractor shall add the airport network information to the data capture database. This network information shall be provided to the contractor to facilitate the opening of ports prior to deployment or pilot testing. The contractor will coordinate with the STIP PMO should any RFCs be needed in support of the port opening.

The contractor shall provide STIP deployment connectivity support. The contractor shall be responsible for monitoring connectivity, monitoring device status, and providing connectivity status reports during each airport deployment.

The contractor shall have processes and procedures in place for keeping customers informed about the status of the deployment, shall be in regular communications with the STIP PMO, OIT, and the STIP Development contractor support to coordinate deployment communications. The contractor shall have help desk support available from 8:00 AM to 5:00 PM (EST), Monday through Friday.

The contractor shall provide afterhours support for software deployments.

The contractor shall provide test support for STIP activities. The support tasks consist of:

5.4.1 Test support – Integration

- Participate in the test IPTs. Provide appropriate inputs and updates.
- Work the test schedule with IPT stakeholders
- Assist in the remediation of test user IDs and password issues with the respective airport POC to ensure they are in place prior to deployment
- Generate and defend the RFC for integration test connection of the TSIF TSE to the SCCB

5.4.2 Test support – Operational Assessment of TSE

- Participate in the test IPTs. Provide appropriate inputs and updates;
- Work the operational assessment schedule with IPT stakeholders;
- Assist in the remediation of user IDs and password issues with the TIP contractor to ensure they are in place prior to the start of test;

- Generate and defend the RFC for operational assessment connection to the SCCB;
- Coordinate TUM training with the OA airport(s);
- Using the dispatch support (unless it is at the TSIF), physically track the TSE connectivity path and note jack/port/switch information on the data capture sheet (typically 4 to 8 TSE units);
- Using the dispatch support (unless it is at the TSIF), physically check of patching from the TSE to the information outlet (jack) and remediate if necessary;
- Using the dispatch support (unless it is at the TSIF), physically patch from the patch panel to the switch.
- Other test support tasks similar to those above.

5.4.3 TSE Deployment Connectivity Support

The contractor shall provide connection support for STIP deployment activities. The connection support tasks consist of:

- Participate in the deployment IPTs. Provide appropriate inputs and updates;
- Work the deployment schedule with IPT stakeholders;
- Assist in the remediation of user IDs and password issues with the TIP contractor to insure they are in place prior to deployment;
- Generate and defend the RFC for connection to the SCCB;
- Work TUM training with each airport;
- Using the dispatch support (unless it is at the TSIF), physically track the TSE connectivity path and note jack/port/switch information and any notes on the data capture sheet;
- Using the dispatch support (unless it is at the TSIF), physically check of patching from the TSE to the information outlet (jack) and remediate if necessary;
- Using the dispatch support (unless it is at the TSIF), physically patch from the patch panel to the switch;
- Activate the connection and confirm by sending at least 2 successful commands to the TSE. (This may be a 2-step process. First confirm the path from the jack to the STIP EM before the TSE arrives/is upgraded, and then confirm connectivity after the STIP upgrade.)
- Provide patch cables as necessary to connect TSE to the information outlet (floor or wall jack) and from the patch panel to switch as required. Patch cables shall match the horizontal infrastructure at that airport, Category 5E or Category 6, and shall be blue in color.
- Provide and coordinate the EMOC and help desk connection activities detailed in the STIP TSE Connectivity SOP.

The contractor shall follow the approved processes outlined in the STIP TSE Connectivity SOP (draft) to establish connectivity to STIP-enabled TSE. Lessons learned shall be incorporated into the document as required.

All connections to TSANet shall be covered by an approved RFC. The STIP TSE Connectivity SOP outlines an approved methodology RFC for STIP-enabled TSE connections.

Connectivity shall be validated by the STIP Help Desk, and a completed data capture sheet (DCS), which includes identifying TSE information and location details, shall be uploaded to the STIP iShare during connection activity, and upon completion of TSE connections. This information will be maintained by the contractor as part of the STIP task order.

Deployment of STIP-enabled and communicating TSE is expected to scale up to approximately 3,600 in the next 12-18 months. The CLIN structure supports incremental increases (250 communicating devices) in the numbers of TSE supported.

5.5 Infrastructure Gap Remediation (IGR)

A contract for Infrastructure Gap Remediation (IGR) at airports is ongoing through September 2015. The IGR contractor is remediating cabling and IT hardware infrastructure gaps for all TSE at each airport location and connect STIP-enabled TSE as they work at airports.

The contractor shall actively participate in the IGR IPTs and support the IGR contractor with back end services (EMOC) for switch connectivity. Coordination and reporting of status for the contractor's scope shall be required at the IPTs and on a weekly/monthly basis. The reports format will be defined at the IPT.

5.6 Operations and Maintenance Dispatch Support

The contractor shall provide dispatch/onsite (airport) O&M services for connectivity related issues. The contractor shall first attempt to diagnose device and/or connectivity issues remotely. If required, the contractor shall dispatch support to tone-test cabling and reconnect STIP-enabled TSE.

The contractor shall dispatch/deploy in a manner most efficient and cost effective to the government. The contactor, for example, will not need to deploy or execute connectivity requirements for fewer than two devices per CAT X or I site per visit at any time. CAT II, III and IV airports may have dispatches scheduled for single TSE connection issues.

6 Task 2 – TSIF Support

The contractor shall provide ongoing lab support at the TSA Systems Integration Facility (TSIF) STIP Lab, located at Ronald Reagan National Airport, Arlington, VA. The support activity includes:

- Requests for on-site support shall be supported within one business day after the request has been received.
- The contractor shall be responsible for Environment setup and configuration activities, which is defined as delivering new or repurposed virtual machines within the existing five Virtual Hosts in the STIP servers.
- Patching shall be performed on the systems and coordination shall be made between the contractor and the systems integrator to avoid a technical conflict with the STIP development efforts.
- OS patching shall be performed on a monthly basis. All patches will follow the TSA approved configuration management\change management process prior to deployment in the TSIF environments.
- This tasking does not require knowledge of STIP application functionality for any application configuration or testing requirements; the STIP development provider will provide these services.

- TSA will provide all equipment and software licenses required for this Task Order.
- Unless otherwise indicated, all services on this Task Order shall be provided at TSIF during TSIF's regular hours of operation.
- Maintenance that impacts the availability of the system during the TSIF's regular hours of operation shall be completed during non-business hours and on weekends.
- The TSIF STIP Lab documentation shall be kept up-to-date.
- The contractor shall be responsible for prepping all TSIF Lab equipment for monthly power outages and recover all TSIF Lab equipment from power outages.

The contractor shall provide level Tier 1, 2 and Tier 3 infrastructure/networking support at the TSIF STIP Lab in the following areas:

- Network connectivity support for TSIF STIP Lab environment
  - TSE connectivity to TSIF STIP Lab network
  - TSE connectivity external to TSIF STIP Lab
  - Support external networking of TSIF STIP Lab
- Backup and recovery activities
- Environment setup and configuration of new environments activities
- Lab workstations maintenance and OS patching

The contractor shall be responsible for monitoring of TSIF STIP hardware software and environment, as well as the installation and setup of replacement or new equipment (desktops or servers).

The contractor shall provide ongoing lab support, including application of patches/security fixes.

The contractor shall support recurring and ad hoc STIP server patch management activities in TSIF STIP Lab environments. Patch management activities include impact analysis, application of patches, coordination with TSA through conference calls and meetings, testing of patches, and developing a test analysis report.

The contractor shall support the following activities and timelines for all applicable STIP servers upon notification to the contractor:

- Quarterly Oracle/WebLogic CPU Testing within 90 calendar days of issuance of Information Security Vulnerability Message.
- Monthly Microsoft Patching within 14 calendar days of issuance of Information Security Vulnerability Message.
- Microsoft Out-of-Cycle patching within 14 calendar days of issuance of Information Security Vulnerability Message.
- Other Information Security Vulnerability Messages pertaining to the STIP applications and servers based on the compliance timeline of the Information Security Vulnerability Message. The timeframe for resolution will be dependent on severity and externally driven deadlines; the government and contractor shall agree upon delivery dates based on impact analysis and a ROM for completion.

- Del 179 STIP TSIF Status Report
- Del 180 Test Analysis Report (TAR)
- Del 181 Patch Impact Analysis

7 Task 6 – Engineering Services

The government anticipates unforeseen work not defined elsewhere in this SOW. This support will be used for such work as:

- Disaster recovery;
- Unique and extended maintenance issues;
- Identifying and documenting recommended engineering fixes or changes;
- High priority activity
- Other unforeseen work.

The contractor shall estimate this work and receive notice to proceed from the COTR in all instances.

8 Task 7 – Program Management

The contractor shall appoint a single point of contact that will serve as the interface between the contractor and the STIP Program Office.

8.1 Program Status Report (Del 182)

The contractor shall report their progress in a monthly (5th of each month) Program Status Report (PSR) for all tickets and SOW tasks:

- Total open and closed trouble tickets per period and by application.
- Total open and closed trouble tickets to date.
- Average open time for trouble tickets
- Ticket aging report by Help Desk trouble ticket type
- TSE connectivity status for operational sites
- Percentage of tickets resolved
- Customer satisfaction summary for the following categories: communication effectiveness, responsiveness, timeliness of resolution, and overall satisfaction.
- ITF and PROD Server Metrics
  - CPU Utilization
  - Memory Utilization
  - SWAP Utilization
  - DB Utilization

The contractor shall track performance metrics to allow the government to track the performance of each task identified in this SOW. These performance metrics shall be included in each Program Status Report for the reporting period, and shall include the following: work performed, problems encountered, pending issues and work planned for the next period.

Additionally, the government reserves the right to request ad hoc reports as deemed necessary for program management. At the time of request, the government and contractor shall agree upon a timeframe for delivery.

- Del 182 Program Status Report (PSR)

8.2 Meetings and Reviews (Del 183)

The contractor shall attend regularly scheduled weekly integrated team status meetings to ensure effective program management, and efficient and effective resolution of problems throughout the life of the contract. These meetings will include the government, and all other government identified contractors.

The contractor shall hold working level meetings, as necessary, known as Technical Interchange Meetings (TIMs). TIMs are specific agenda driven and the agenda for each TIM is mutually agreed upon between the government and contractor. All TIMs require government approval. The contractor shall provide meeting minutes within three (3) business days from the date the meeting occurred.

- Del 183 TIM Meeting Minutes

8.3 Deliverable Schedule

The following table identifies the deliverables that will be required for this SOW. While the content and definition are defined throughout the SOW, this table outlines the format of these deliverables and the estimated due date of the deliverable. All time periods with days are to be considered business days.

Task	Deliverable No.	Deliverable Title	Format/ Media	Estimated Due Date
2	Del 179	STIP TSIF Status Report	MS Word	5th business day of each month
2	Del 180	Test Analysis Report (TAR)	MS Word	As required
2	Del 181	Patch Impact Analysis	MS Word	As required
7	Del 182	Program Status Report (PSR)	MS Word	5th business day of each month
7	Del 183	Technical Interchange Meeting(TIM)	MS Word	As necessary
7	Del 184	Post Award Conference Meeting Minutes	MS Word	5 days after meeting
7	Del 185	Transition Plan (Phase-in)	MS Word/Excel	Two weeks after award
7	Del 186	Transition Plan (Phase-out)	MS Word/Excel	120 business days prior to end of contract

Figure 5: Deliverable Schedule

8.4 Post Award Conference

The government will hold a post-award conference at a location designated by the contracting officer within ten (10) business days after the STIP requirement is awarded. At the post-award conference, the contractor shall present their understanding of the STIP requirement and identify any issues or questions about the execution. The government will designate conference attendees and identify any unique conference support requirements. The contractor shall provide the minutes for the conference within five (5) business days after the post award conference.

- DEL 184 Post Award Conference Meeting Minutes

9 Miscellaneous

STIP System Status Statements:

1. The current STIP and associated supporting systems have been designed and implemented according to all Federal, DHS and TSA security policies and guidelines.
2. The STIP program office is responsible for any outstanding plan of action and milestones (POA&Ms) or findings associated with the current STIP and supporting systems to include both backend server infrastructure and the TSA security equipment (TSE) devices.
3. The contractor shall be responsible for SOC support and CSIRT incident response up to the switch connecting to the TSA security equipment (TSE) device. Any additional support needed will then be handed off to the appropriate third-party vendor.

Security Requirements Not Covered under STIP SOW:

1. Configuration of the TSA security equipment (TSE) devices.
2. Operating system patches and updates (to include security patches and updates) for the TSA security equipment (TSE) devices.
3. Antivirus support for TSE. Vulnerability scanning of the TSA TSE.
4. Remediation of any security finding or POA&Ms for the TSA TSE.

Intellectual Property: All contractor developed processes and procedures and other forms of intellectual property first developed under this task order shall be considered government property.

INTELLECTUAL PROPERTY (DELIVERABLE) - Data required to be delivered under this task order, that could be deemed technical data under the clause FAR 52.227-14, Rights in Data – General, if it were delivered in written form, shall not lose its status as technical data because access by the government, or delivery by the contractor, is by electronic means. All configuration work undertaken by the contractor and recorded or uploaded into or installed upon any government system (including development, test, production, and failover environments) under this or any related or predecessor contract, is deemed to have been delivered to the government and shall be the property of the government. All rights of the parties in these technical data deliverables shall be as specified in the clause Rights in Data – General.

10 Transition Activities

The contractor recognizes that the work and services provided under this requirement are vital to the TSA mission and must be maintained without interruption, both at the commencement and expiration of this contract. It is therefore understood and further agreed in recognition of the below:

(a) At the end of the period of performance, the contractor shall cooperate with a successor contractor or the government. After selection by the government of any successor contractor, the contractor and such successor contractor shall jointly prepare mutual detailed plans for phase-out and phase-in operations. Such plans shall specify a training and orientation program for the successor contractor to cover each phase of the scope of work covered by the contract. A proposed date by which the successor contractor will assume responsibility for such work shall be established. The contractor shall assume full responsibility for such work until assumption thereof by the successor contractor. Execution of the proposed plan or any part thereof shall be accomplished in accordance with the contracting officer's direction and approval.

(b) The contractor shall provide a transition plan for taking over the duties and responsibilities of this contract that will cover the training and knowledge transfer from the outgoing to the incoming contractor.

(c) The conversion of the STIP Help Desk phone number and email address shall remain separate and shall be merged with the TSA SPOC number at a mutually agreed upon schedule by the TSA COR and the contractor.

- Del 185 Transition Plan (Phase-in)
- Del 186 Transition Plan (Phase-out)

11 Place of Performance

The work shall be performed at the contractor and TSA sites.

Local travel within the DC metropolitan area is required. The contractor shall attend meetings at TSA Headquarters in Arlington, VA, and may travel to the TSIF location for the execution of tasks.

12 Travel and ODCs

Non-dispatch travel, if required, shall be pre-approved by the government prior to expenditure. All travel requests shall include the nature, purpose, and travel details including estimated dollar amount. Approved travel subsistence reimbursements will be authorized under the rates and conditions under the Federal Travel Regulations.

Local travel, defined as within 50 miles of the home location, is not reimbursable.

Travel and ODCs are based on a not-to-exceed (NTE) amount. All materials purchased by the contractor under this item become property of the federal government. The contractor shall notify the contracting officer in writing when the costs exceed 75 percent of the NTE value on the travel and ODC CLIN.

13 ITIP Bridge Task Order Performance Work Statement

The contractor shall perform the requirements as outlined in this Statement of Work. In addition, the leveraged services will be performed in accordance with Section 3 of the Performance Work Statement (PWS) of the Information Technology Infrastructure Program (ITIP) Continuation of Services Task Order, HSTS03-15-J-CIO656, under the Enterprise-Wide Acquisition Gateway Leading Solutions II (EAGLE II) indefinite delivery, indefinite quantity (IDIQ) contract HSHQDC-13-D-E2090.