OFFICE OF INSPECTOR GENERAL

IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted)

Homeland Security

May 9, 2016

OIG-16-87

~~SENSITIVE SECURITY INFORMATION~~

DHS OIG Highlights

IT Management Challenges Continue in TSA's Security Technology Integrated Program

May 9, 2016

Why We Did This Audit

We previously reported on deficiencies in information technology (IT) security controls of the Security Technology Integrated Program (STIP), a data management system that connects airport transportation security equipment (TSE) to servers. We conducted this audit to assess the current extent of the deficiencies and the actions the Transportation Security Administration (TSA) has taken to address them.

What We Recommend

We are making 11 recommendations to TSA to improve the control, security, and functionality of STIP IT assets.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

As described in our prior reports on this issue, numerous deficiencies continue in STIP IT security controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with departmental guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA did not effectively manage all IT components of STIP as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSE from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.

Recently, TSA has taken steps to resolve these STIP deficiencies. For example, according to a TSA staff member, system owners may no longer prevent the implementation of required software patches. TSA is also working to include cybersecurity requirements in the procurement process. However, more time is needed to determine the effectiveness of these improvement initiatives.

Agency Response

The agency concurred with all 11 recommendations. All recommendations are resolved and open, except for recommendation 5, which is unresolved and open.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 9, 2016

MEMORANDUM FOR: The Honorable Peter Neffenger
Administrator
Transportation Security Administration

FROM: John Roth
Inspector General

SUBJECT: *IT Management Challenges Continue in TSA's Security Technology Integrated Program*

Attached for your information is our final report, *IT Management Challenges Continue in TSA's Security Technology Integrated Program.* We incorporated the formal comments from the Transportation Security Administration (TSA) in the final report.

The report contains 11 recommendations aimed at improving security controls for TSA's Security Technology Integrated Program systems. Your office concurred with all of the recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Based on information provided in your response to the draft report, we consider all 11 recommendations resolved and open, except for recommendation 5, which is unresolved and open. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General, Office of Information Technology Audits, at (202) 254-4041.

Attachment

Table of Contents

Appendixes

Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
DC1	Data Center 1
DC2	Data Center 2
EDS	explosive detection system
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSC	Office of Security Capabilities
SOO	statement of objectives
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSE	transportation security equipment

Background

The Transportation Security Administration's (TSA) mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. This mission involves passenger and baggage screening and threat detection through the use of Explosive Trace Detectors, Explosive Detection Systems, Advanced Technology X-ray, Advanced Imaging Technology, and Credential Authentication Technology. TSA's Security Technology Integrated Program (STIP) enables the remote management of this transportation security equipment (TSE) by connecting it to a centralized server that supports data management, aids threat response, and facilitates equipment maintenance, including automated deployment of software and configuration changes. This significantly reduces the time needed to deploy critical software updates and configuration changes in response to emerging threats, for example, within and amongst the screening machines and STIP central servers. As such, STIP has been designated a mission-essential program.

The Office of Security Capabilities (OSC) is responsible for the Passenger Screening Program, the Electronic Baggage Screening Program, and STIP. OSC's mission is to safeguard our Nation's transportation systems through the qualification and delivery of innovative security capabilities and solutions. STIP stakeholders include TSA Headquarters, OSC, Office of Information Technology, Office of Intelligence and Analysis, airport leadership/management, original equipment manufacturers, and maintenance service providers.

As a result of our prior audits of information technology (IT) security controls at selected U.S. airports, we repeatedly reported IT security control deficiencies associated with STIP. Across the various locations, we found instances where:

- TSA was not scanning STIP servers for technical vulnerabilities.
- Temperatures in STIP server rooms exceeded Department of Homeland Security (DHS) guidelines.
- Non-DHS airport employees had access to STIP server rooms.
- TSA had not implemented a process to report STIP-related computer security incidents to the TSA Security Operations Center.

- STIP servers were not included in information systems security plans.
- TSA had not established interconnection security agreements to document STIP connections to non-DHS baggage handling systems.
- STIP servers were using an operating system that was no longer supported by the vendor.
- STIP information security documentation inadequately identified the risks inherent in operating STIP.

Following is the list of our prior reports in which we reported these STIP IT control deficiencies.

- *Technical Security Evaluation of DHS Components at O'Hare Airport,* OIG-12-45, March 2012
- *Technical Security Evaluation of DHS Activities at Hartsfield-Jackson Atlanta International Airport*, OIG-13-104, July 2013
- *Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport*, OIG-14-132, September 2014
- *Audit of Security Controls for DHS Information Technology Systems at San Francisco International Airport*, OIG-15-88, May 2015

We conducted this audit at DHS data centers and the Orlando International Airport to further assess the extent of STIP deficiencies and the actions the TSA has taken to address them.

Results of Audit

As described in our prior reports on this issue, numerous deficiencies continue in STIP information technology security controls, including unpatched software and inadequate contractor oversight. This occurred because TSA typically has not managed STIP equipment in compliance with DHS guidelines regarding sensitive IT systems. Failure to comply with these guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of TSA's automated explosive, passenger, and baggage screening programs.

TSA also has not effectively managed STIP servers as IT investments. Based on senior-level TSA guidance, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts. This promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP servers from the network. TSA also did not report all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.

Recently, TSA has taken significant steps to resolve these STIP deficiencies. For example, according to a TSA staff member, system owners may no longer prevent implementation of software patches due to concerns with system performance. TSA is also working to include cybersecurity requirements in the equipment procurement process. However, more time is needed to determine the effectiveness of these improvement initiatives.

We are making 11 recommendations to TSA to address STIP IT security control and cost reporting deficiencies.

STIP IT Security Control Deficiencies

Contrary to DHS guidelines for managing sensitive IT systems, we identified a pattern of deficiencies in STIP information technology security controls: server software vulnerabilities, a lack of an established disaster recovery capability, physical security deficiencies, and inadequate vulnerability reporting. Typically, TSA did not ensure that basic security requirements were integrated into the software and procurement life cycle for STIP project development. IT security controls and testing requirements also were not included in STIP server contracts. Failure to comply with DHS' sensitive systems guidelines increases

the risk that baggage screening equipment will not operate as intended, resulting in potential loss of confidentiality, integrity, and availability of the TSA's automated explosive, passenger, and baggage screening programs.

STIP Server Software Deficiencies

STIP server software vulnerabilities included unpatched software, unsupported operating systems, and a lack of adequate contractor oversight. These software vulnerabilities were identified in August and September 2015, when we observed TSA staff as they scanned STIP servers located at DHS Data Center 1 (DC1), DHS Data Center 2 (DC2), and the Orlando International Airport. The technical scans detected a total of 12,282 high vulnerabilities on 71 of the 74 servers tested.[1] The scans detected no vulnerabilities on the remaining three servers. See appendix E for a breakdown of vulnerabilities by location.

Of the 12,282 high server vulnerabilities, 9,263 (75.4 percent) were associated with [redacted] For example, [redacted] These vulnerabilities could adversely affect the availability and the reliability of STIP. According to TSA staff, software patches for [redacted] applications were not installed because TSA system owners were concerned that the patches would degrade the performance of their systems. Other vulnerabilities rated 'high' by the scanning software but unrelated to these two applications have been known for years—one such vulnerability dates back to 1999. These vulnerabilities include [redacted]

Operating systems on a number of the STIP servers tested did not meet Departmental requirements. For example, 8 of the 74 servers tested (10.8 percent) used an operating system for which the minimum security configuration guidance had not been established. Further, 47 of the 74 servers

[1] The scanning software used for this audit scores vulnerabilities on a scale of 0 to 10, which is based on the Forum of Incident Response and Security Teams' Common Vulnerability Scoring System. Within this system, the more easily a vulnerability can be exploited, the higher the vulnerability score. For this report, vulnerabilities scored over 6.9 are considered to be 'high.'

(63.5 percent) used [redacted]

One of the causes for the software and operating system vulnerabilities was that TSA previously did not include IT security requirements in STIP server contracts, especially regarding the use of DHS-approved operating systems. Further, TSA did not ensure in its contracts that TSA staff would have administrator rights, such as user IDs and passwords, to access and maintain security on STIP airport servers. [redacted] TSA lacked the policies or procedures and the oversight mechanisms needed to [redacted]

Another cause for the software vulnerabilities was that TSA did not test IT security controls on STIP airport servers or IT components of TSEs prior to equipment deployment. Individual tests of the functionality of each piece of TSE are performed at the Transportation Security Laboratory in Atlantic City, NJ. At this location, TSA tested these devices as standalone pieces of equipment, even though some were deployed at airports as part of local area networks LAN. At the Transportation Security Integration Facility in Arlington, VA, TSA tested the functionality of TSE servers, data storage devices, and local area network configurations prior to their deployment at airports. However, TSA did not test the IT security controls on these devices at either location.

The failure to timely update STIP server software was contrary to requirements of the *DHS 4300A Sensitive Systems Handbook* Version 9.1 (July 2012) at p. 53:

- Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management message published by the DHS Enterprise Operations Center.

The use of operating systems lacking departmental baseline security configuration guidance was also contrary to the requirements of the *DHS 4300A Sensitive Systems Handbook,* Version 9.1 (July 2012) at p. 152:

- Components shall ensure that DHS information systems follow configuration guidance provided by the DHS Chief Information Security Officer (CISO).

TSA's use of the older Windows Server 2008 operating system was not in compliance with *DHS 4300A Sensitive Systems Handbook, Enclosure 1, Windows Server 2008 Configuration Guidance*, Version 2015.7, July 2015, p. 1:

- Within DHS, Windows Server 2008 should be upgraded to Windows Server 2012.

Further, TSA's lack of control of STIP server software and operating systems was not in compliance with *DHS 4300A Sensitive Systems Handbook,* Version 9.1 (July 2012) at p. 152:

- Components shall limit access to system software and hardware to authorized personnel.

- Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.

- Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.

- If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.

Failure to comply with DHS' sensitive systems guidelines increases the risk that baggage screening equipment will not operate as intended, resulting in

potential loss of confidentiality, integrity, and availability of the TSA's automated explosive, passenger, and baggage screening programs.

Inadequate Disaster Recovery Capability

TSA has not established an effective disaster recovery capability for STIP servers residing at DC2. Although the TSA *STIP Contingency Plan* identified DC1 as the alternate STIP processing site in case of disasters, the ability to restore STIP processing at DC1 was not yet operational at the time of our audit. For example, there was insufficient STIP server processing capacity at DC1 to provide full operational capability.

In June 2015, TSA's Chief Information Officer (CIO) granted STIP a 7-month authorization to operate. The CIO also noted that STIP was a mission-essential system and that the overall Federal Information Processing Standards security categorization for STIP was high. Based on this security categorization, an alternative processing site for STIP was needed to ensure that managers administering airport security equipment were able to make TSE configuration changes and track TSE status, error conditions, and performance.

According to *DHS 4300A Sensitive Systems Handbook,* Version 9.1 (July 2012) at p. 67:

- Components shall ensure that an established alternate site is available for systems with high impact availability. Resources for establishing an alternate site shall be identified and made available for systems assessed as high impact for availability.

Without an established STIP disaster recovery capability, TSA's managers may not be able to adequately track TSE baggage and passenger screening performance if DC2 becomes inaccessible due to a natural or manmade disaster such as a telecommunications or power outage. In such instances, TSA's ability to fulfill its mission of protecting the Nation's transportation system and freedom of movement of people and commerce could be significantly impacted.

Physical Security and Environmental Control Deficiencies

TSA did not adequately secure all STIP switches operating at Orlando International Airport. For example, some of the STIP switches located in a shared space were not contained within a locked cabinet. As a result, non-DHS

personnel with access to this room had the potential to steal, modify, damage, or destroy these STIP switches and thereby adversely impact TSA's local area network operations.

A member of TSA staff stated the lack of physical security for the TSA switches was due to incomplete inventory, including locations, of STIP switches at Orlando International Airport. As such, TSA staff had not previously reviewed the physical security controls for all of the STIP switches at this airport as required.

As stipulated in the *DHS 4300A Sensitive Systems Handbook,* Version 9.1 (July 2012) at pp. 104 and 107:

- Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.

These physical security deficiencies made it possible for non-authorized individuals to gain access and potentially damage or modify TSA IT equipment.

Inadequate Vulnerability Reporting

TSA has provided to the Department the required vulnerability assessment reports for only 38 of the 74 (51 percent) STIP servers. Detailed vulnerability assessment scan schedules and results were to be provided as part of the DHS Information Security Vulnerability Management program. This comprehensive department-wide program of vulnerability alert, assessment, remediation, and reporting is intended to ensure effective, continuous identification and management of computer security vulnerabilities, risks, and threats, and to track vulnerability mitigation through to resolution.

However, STIP servers at Orlando International Airport could not be scanned for vulnerabilities from a remote location. TSA had not established a procedure for providing the necessary vulnerability scans and reports for these eight servers.

According to *DHS Sensitive Systems Handbook 4300A*, Attachment O, *Vulnerability Management Program,* Version 9.1 (July 2012) at p. 5:

- Detailed vulnerability assessment scan schedules and results must be provided to the DHS Vulnerability Management Branch in order to satisfy *Federal Information Security Management Act*, Public Law 107–347 of 2002, requirements for enterprise-wide security situational awareness of assets and risks.[2]

Vulnerability reporting is the process that helps identify and validate the number of systems that comply or do not comply with DHS security guidance. Failure to report server vulnerabilities to DHS prevents leadership from adequately monitoring overall system compliance with DHS security policies.

We recommend that the TSA CIO and Assistant Administrator for OSC jointly:

Recommendation 1: Ensure that IT security controls are included in STIP system design and implementation so that STIP servers are not deployed with known technical vulnerabilities.

Recommendation 2: Ensure that STIP servers use approved operating systems for which the Department has established minimum security baseline configuration guidance.

Recommendation 3: Ensure that STIP servers have the latest software patches installed so that identified vulnerabilities will not be exploited.

Recommendation 4: Ensure that IT security testing is performed so that STIP servers are not deployed with known technical vulnerabilities.

Recommendation 5: Ensure that authorized TSA staff obtain and change administrator passwords for all STIP servers at airports so that contractors no longer have full control over this equipment at airports.

Recommendation 6: Implement a contractor oversight process so that only authorized and approved software, along with timely updates, is installed on STIP airport servers.

[2] *Federal Information Security Management Act,* Public Law 107–347 of 2002, was amended in December 2014 by the *Federal Information Security Modernization Act of 2014*, Public Law 113–283.

Recommendation 7: Inventory all locations at Orlando International Airport housing STIP servers and switches and ensure that these locations comply with DHS policy concerning physical security controls.

Recommendation 8: Ensure an adequate operational recovery capability for STIP servers at DC1 in case DC2 becomes inaccessible.

Recommendation 9: Establish a process for providing STIP server vulnerability assessment reports to the Department so that DHS leadership may adequately monitor system compliance capability.

Agency Comments and Office of Inspector General (OIG) Analysis

We obtained written comments on a draft of this report from the TSA Administrator. We have included a copy of the comments in their entirety in appendix C. TSA concurred with all of the recommendations. We have reviewed the Administrator's comments, as well as the technical comments previously submitted under separate cover, and made changes to the report as appropriate. Following is our evaluation of the Administrator's comments, as well as his response to each recommendation in the draft report provided for agency review and comment.

Agency Comments to Recommendation 1:

TSA concurs with this recommendation. TSA has developed a Cybersecurity Statement of Objective (SOO) inclusive of critical requirement to bring legacy TSEs — including the explosive detection system (EDS) servers — into compliance with IT security controls mandated by DHS. Additionally, future procurements must include these requirements. TSA has also created a formal Cybersecurity Management Framework and Plan that lays out an organizational framework and strategy to oversee the implementation of IT Security requirements onto legacy TSEs. TSA will issue the Cybersecurity SOO to current TSE vendors by the end of August 2016. The implementation of the requirements on the current TSEs will be dependent on the cost/schedule proposed by the vendors and TSA's availability of the funds to execute the cybersecurity remediation contracts. TSA has initially estimated that $4.66 million in future year funding is needed to remediate the current fleet of legacy TSEs and provide the necessary support and staff to manage the operations and maintenance needed to meet the ongoing cybersecurity

requirements. TSA estimates that the Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 1:

TSA's plans satisfy the intent of this recommendation. However, implementation of this recommendation requires the issuance of the SOO, new procurements, and new support staff. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 2:

TSA concurs with this recommendation. In April 2015, TSA began to catalogue and disconnect any TSA TSE not running a supported operating system. TSA has made progress to replace outdated Windows operating systems and will continue its effort until TSEs run on supported operating systems. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts. TSA is working with vendors to remediate TSEs with outdated operating systems that cannot be entirely removed from the screening process due to their criticality to mission effectiveness. TSA will investigate and put into place compensating security controls as an interim risk mitigation measure while outdated operating systems are phased out of the enterprise. TSA has initiated comprehensive market research to identify the latest cybersecurity tools that can be applied to the endpoint device, as well as network infrastructure. This market research will be completed by the end of May 2016. TSA will then engage with identified vendors to collaborate on proofs of concept to validate requirements and capabilities that can transition to an enterprise-wide implementation. The Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 2:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation includes using only approved operating systems on STIP servers. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 3:

TSA concurs with this recommendation. TSA has taken steps to identify and implement IT security controls to position the agency for future defense against cybersecurity attacks on the TSEs. In addition, the Cybersecurity SOO contains requirements around Operating System Currency/Security Patching. Implementation will vary and is dependent on each vendor and TSA's ability to fund those efforts. TSEs are required to be tested for operating system patch compatibility before the patches are installed. According to TSA, such patches can only be completed by the vendors due to the proprietary nature of their system. Keeping these constraints in mind, TSA is developing a process map to remotely patch TSEs. TSA estimates that the market research will be completed by May 2016 and the Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 3:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation includes using only approved operating systems, with the latest required software patches, on STIP servers. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 4:

TSA concurs with this recommendation. TSA has already mandated IT Security Scanning by engineers from the TSA Office of Information Technology Information Assurance Division during integration testing of STIP EDS servers and any updates software images. Findings are translated into formal plan of actions and milestones for IT Security remediation and assigned different levels of urgency from critical to low and associated timeframes to correct. Timely remediation is also one of the key requirements embedded in the TSA Cybersecurity SOO that is being issued to technology vendors. TSA estimates that the governance document mandating scanning of STIP servers will be changed by June 30, 2016.

OIG Analysis of Agency Comments to Recommendation 4:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation includes using only approved operating systems, with the latest required software patches on STIP servers, in addition to scanning these servers. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 5:

TSA concurs with this recommendation. TSA Cybersecurity SOO includes requiring vendors with access to the TSEs to be adjudicated through the Personal Identity Verification card validation system and controlled by TSA through the STIP. In addition, card holders would also have to undergo a TSA-mandated vetting process in order to be issued a Personal Identity Verification card. This means that everyone — including technology vendors and maintenance contractors — will have been vetted and would have to log into specific TSEs using their cards. TSA Cybersecurity SOO mandates that TSA obtain administrative access to conduct remote security scanning of TSEs every 72 hours — per DHS mandate — and receive log files in near real-time. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts. TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure as TSA staff explores the potential operational impacts to Personal Identity Verification card implementation. TSA estimates that the governance document mandating scanning of STIP servers will be changed by June 30, 2016.

OIG Analysis of Agency Comments to Recommendation 5:

TSA has not provided the steps to obtain and change administrator passwords for STIP servers at airports. This recommendation is considered unresolved and will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 6:

TSA concurs with this recommendation. TSA will review logical and physical access controls as they apply to TSEs, including an audit of privileged user access. This effort will also include analyzing maintenance and development contracts to ensure necessary controls are contractually in place to prevent unauthorized use of these systems. Once TSA Cybersecurity SOO requirements are implemented, automated configuration audits will be possible to identify any unauthorized deviation from approved configuration baselines for TSEs. TSA estimates that the Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 6:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation includes the implementation of an oversight process, such as the identified automated configuration process. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 7:

TSA concurs with this recommendation. TSA is currently planning an asset inventory effort to identify and validate the locations of TSA-owned IT equipment attached to TSEs, including STIP EDS servers and associated peripherals. This effort will serve to address the immediate needs of identifying locations and equipment, and will provide information for improving the asset management process. The primary focus will be on airports that contain STIP servers and peripherals. The initial phase will involve the National Capital Region airports and will conclude by July 31, 2016. Based on the lessons learned from the initial phase, the timeline for an enterprise-wide asset inventory effort for TSE-related IT equipment will be established.

OIG Analysis of Agency Comments to Recommendation 7:

TSA is currently planning to conduct an inventory to identify the airport locations containing STIP assets. This inventory will first be conducted in the National Capital Region. TSA has not provided the schedule for inventorying STIP locations at Orlando International Airport. Therefore, this

recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 8:

TSA concurs with this recommendation. TSA will conduct an analysis to determine the level of effort necessary to create full operational recovery capabilities in an alternate location for the STIP servers presently operating in DC2. DC1 and the Cloud are an option, but TSA will identify other locations that might be more cost effective while delivering the same recovery capability. A proposed solution and analysis of its related level of effort will be completed by September 30, 2016. The implementation of the solution will depend on the availability of funds and acquisition of the engineering services required.

OIG Analysis of Agency Comments to Recommendation 8:

TSA plans to analyze the feasibility of creating a full operational recovery capability at an alternative location. However, TSA has not provided the schedule for implanting the selected capability. This recommendation will be remain resolved and open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 9:

TSA concurs with this recommendation. TSA's Office of Information Technology's Information Assurance Division already provides vulnerability assessments reports for STIP data center servers. TSA will review any gaps in this reporting and ensure that the reports are provided for all applicable STIP servers in the data center. Manual scanning is required for unconnected STIP EDS servers at the airport that are in their currently unconnected state. The aforementioned TSA Cybersecurity SOO mandates that TSA obtain administration access to conduct remote security scanning of TSEs every 72 hours to identify any compliance gaps. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts. TSA estimates that the Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 9:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation includes scanning these servers and providing the scanning results to the Department. Until TSA provides documentation that vulnerability assessment reports are provided to the Department, this recommendation will be remain resolved and open.

IT Components of STIP Not Effectively Managed as IT Investments

TSA did not effectively manage all IT components of STIP as IT investments. Based on guidance from the TSA Associate Administrator, TSA officials did not designate these assets as IT equipment. As such, TSA did not ensure that IT security requirements were included in STIP procurement contracts, which promoted the use of unsupported operating systems that created security concerns and forced TSA to disconnect STIP TSEs from the network. TSA also did not identify all STIP IT costs in its annual budgets, hindering the agency from effectively managing and evaluating the benefits and costs of STIP.

TSA Did Not Designate All STIP Equipment as IT Assets

Based on a March 2005 decision memo, *Determining IT versus Non-IT Programs*, that placed passenger and baggage handling IT systems within STIP under total control of TSA CIO, TSA did not designate STIP IT equipment at airports as IT assets. (See appendix D for a copy of the memo.) TSA staff referenced a statement in the memo that "[t]he TSA Passenger Screening Program (Aviation) shall be designated as a non-IT program." However, TSA staff disregarded another statement in the memo recognizing that "almost all non-IT programs have an IT component to them" and must be under the full purview of TSA CIO, particularly with regard to investment control and project oversight.

Staff we interviewed made assertions that there was no STIP IT at airports contrary to a TSA position established in response to a prior OIG report.[3] Specifically, in response to our October 2007 report recommendation 1, the then-Assistant Secretary of TSA concurred that IT components and associated costs of the explosive, baggage, and passenger screening systems would be included in the STIP.

[3] *Information Technology Management Needs to Be Strengthened at the Transportation Security Administration*, OIG-08-07, October 2007.

DHS Sensitive Systems Handbook 4300A, Version 9.1 (July 2012) at p. 4, defines what constitutes IT equipment within the Department as follows:

- IT is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency.

- The term IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Given their interpretation of the March 2005 decision memo, TSA budget staff were coding the costs of STIP airport servers as 'Explosive Detection Machine Equipment – Capital' rather than IT assets in accordance with the Handbook 4300A guidance. During a discussion on this issue, TSA budget and finance staff members stated that they would have used standard IT budget object codes if STIP airport servers had been identified in TSA's contracts as IT assets. Because this was not done, budget and finance staff had to designate the equipment using other non-IT budget object codes, which meant that the IT equipment was not subject to the appropriate IT controls and financial oversight.

IT Security Controls Not Included in TSE Procurement Contracts

Because TSA officials did not designate STIP equipment at airports as IT assets, they did not ensure that IT security requirements were included in TSE procurement contracts. According to *DHS Sensitive Systems Handbook 4300A*, Version 9.1 (July 2012) at p. 34, information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved to the maximum extent possible in all aspects of the acquisition process, including drafting contracts, and procurement documents.

TSA's failure to establish IT security requirements in TSE procurement contracts, as required, promotes the use of unsupported operating systems at airports. TSA deployed the unsupported operating systems without first testing the IT security controls on them to ensure they were adequate. For example, some TSEs were using obsolete Windows operating systems that were no longer supported by Microsoft, leaving them open to potential vulnerabilities. By

August 31, 2015, TSA had to disconnect every TSE from its network due to IT security concerns created by the unsupported operating systems. As of December 2015 at the end of our field work, the TSEs were still disconnected, hindering TSA from remotely maintaining and managing the configuration of these devices. This situation also caused STIP to miss project milestones to network 16,000 TSEs located at 450 airports nationwide by the end of fiscal year 2013. According to TSA CISO, the component will evaluate the cybersecurity operational risk of all TSEs prior to reconnecting to them to the TSA network in the future.

TSA Was Not Reporting All IT Expenses Related to STIP

Because TSA did not designate TSE at airports as IT assets, TSA also did not adequately identify all STIP-related IT expenses in its annual budget submissions. According to TSA's August 2014 STIP budget submission, total development, maintenance, and enhancement costs of STIP were $66.5 million through fiscal year 2014. However, this budget submission only included costs related to STIP IT assets at the DHS data centers. The costs of STIP servers at all airports, as well as the contractors' cost to network all airport TSEs, were not included in TSA's STIP budget submission. The excluded costs of the eight STIP servers at Orlando International Airport that we evaluated amounted to nearly $124,000.

TSA staff continued to deny that STIP airport servers or IT components of TSEs were IT assets, just as they did during our recent evaluations of airport IT security controls. For example, in our IT security control audit report regarding Chicago O'Hare International Airport, TSA provided IT diagrams that excluded STIP airport servers.[4] Similarly, during our audit of IT security controls at Dallas/Fort Worth International Airport, we noted that STIP airport servers were missing from the STIP systems security plan.[5] During this period, some TSA staff would occasionally tell OIG auditors that STIP airport servers were not servers at all, but were part of the airport screening equipment. In TSA expenditure documents, STIP airport servers were listed as "Explosive Detection Machine Equipment – Capital."

TSA's failure to categorize STIP airport servers as IT equipment resulted in inaccurate STIP IT cost reporting. This was contrary to Office of Management

[4] *Technical Security Evaluation of DHS Components at O'Hare Airport*, OIG-12-45, March 2012
[5] *Audit of Security Controls for DHS Information Technology Systems at Dallas/Fort Worth International Airport*, OIG-14-132, September 2014

and Budget's (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget*, July 2014 – Revised November 2014, Section 55.6, p. 3, guidance that agency reporting of its IT Portfolio should include all of its annual IT costs. Additionally, according to OMB's *FY 2017 IT Budget – Capital Planning Guidance*, Revised June 2015, p. 3, to the extent that OMB or the agency CIO determine data reported to the IT Dashboard is not timely or reliable, the CIO (in consultation with the agency head) must notify OMB through the Integrated Data Collection and establish within 30 days of this determination an improvement program to address the deficiencies.

Failure to adequately report expenses for all STIP IT also prevented TSA, Departmental leadership, and OMB from effectively managing and evaluating the benefits and costs of STIP IT in accordance with the DHS *Capital Planning and Investment Control (CPIC) Guidance*, Version 7.1, August 2010, pp. i, 4, 9, and 29. The DHS CPIC process integrates strategic planning, enterprise architecture, privacy, security, budgeting, portfolio management, procurement, risk management, and acquisition management of capital assets. In the process, both IT and non-IT investments are continually monitored and evaluated to ensure each investment is well managed, cost effective, and supports the mission and strategic goals of the Department. The primary product of the CPIC process is the OMB Circular A-11 defined Exhibit 300. The Exhibit 300 encompasses many investment details, including cost, schedule, milestones, and resources. To the extent that this information is incomplete, the agency and OMB are hindered from accurately reviewing and evaluating the agency's IT spending and also making comparisons across the Federal Government.

We recommend that the TSA CIO and Assistant Administrator for OSC jointly:

Recommendation 10: Ensure that IT security requirements are included in equipment procurement contracts for IT components of STIP and passenger and checked baggage screening equipment as required.

Recommendation 11: Institute controls so that all IT costs associated with STIP are accurately captured and reported in annual budget submissions as required.

Agency Comments and OIG Analysis

Agency Comments to Recommendation 10:

TSA concurs with this recommendation. TSA will specify the nine cybersecurity requirements that must be met by various vendors' TSEs prior to connection to TSANet. TSA will investigate and put into place compensating security controls as an interim risk mitigation measure as noncompliant TSEs are phased out of the enterprise. While TSA will work closely with vendors to implement these requirements on legacy and future TSEs, TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure as noncompliant TSEs are phased out of the enterprise. The comprehensive market research about the latest cybersecurity tools as well as network infrastructure that will best mitigate cybersecurity risk will be completed by the end of May 2016. TSA will then engage with vendors to collaborate on Proofs of Concept to validate requirements and capabilities to transition to an enterprise-wide implementation. TSA estimates that the market research will be completed by May 2016 and the Cybersecurity SOO will be issued to all vendors by August 31, 2016.

OIG Analysis of Agency Comments to Recommendation 10:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation requires the issuance of the SOO as well as new or updated procurements. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 11:

TSA concurs with this recommendation. TSA acknowledges that IT cost should be accurately tracked and reported. According to TSA, current policy framework requires all programs be designated IT or non-IT. Therefore, TSA would have to redesignate the Passenger Screening Program and Electronic Baggage Screening Programs (both Non-IT DHS Level I Acquisition Programs) as IT programs in order to meet the recommendation. This redesignation would impose substantial programmatic and cost burdens on these programs, as well as personnel suitability constraints on current and future TSE procurement and maintenance contracts. This would be disruptive to current security operations and impact TSA's mission readiness.

TSA proposes creating an alternate program designation for these programs that have both IT and non-IT elements. The handling of these "hybrid" and or "mixed" programs will require program-specific tailoring of governance that considers the oversight and reporting requirements of DHS and TSA. TSA will investigate how costs for TSEs can be best captured into IT and non-IT components to inform cost reporting, budget submissions, and the Capital Planning Investment and Control process. TSA plans to establish a working group by the end of April 2016 to examine its governance options and submit recommendations to the DHS and TSA leadership by the September 30, 2016.

OIG Analysis of Agency Comments to Recommendation 11:

TSA's plans satisfy the intent of this recommendation. However, complete implementation of this recommendation requires the capture and reporting of all IT costs associated with STIP. This recommendation is considered resolved but will remain open until TSA provides supporting documentation that all corrective actions are completed.

TSA Actions to Resolve STIP IT Control Deficiencies

Recently, TSA has taken significant steps to address STIP IT control deficiencies. A number of these steps were taken in response to recommendations in prior OIG reports. These steps include immediate actions to address current cybersecurity issues as well as develop plans to address systemic issues. For example,

- TSA has placed the STIP servers at its data centers within the boundaries of the Infrastructure Cores Services system—the same system that contains other TSA servers. This action may allow TSA to better manage the IT security of the STIP servers at the data centers. In our view, the STIP servers at the airports would benefit from being placed within the same boundaries.

- According to a TSA staff member, TSA will no longer allow system owners to prevent the installation of system software patches. These changes should allow TSA to ensure that system software is updated timely.

- TSA has developed a plan to locate STIP support equipment, including servers and switches, at all airports, as a means of addressing the recurring physical security and environmental controls deficiencies. This

plan should allow TSA to prioritize locations where physical security enhancements are required.

- TSA has expanded the security boundaries of the STIP system to include all STIP TSE at airports. This action was taken in conjunction with re-authorizing the STIP to operate. As a result of this re-authorization action, TSA also upgraded the STIP to a mission critical system. This designation should allow TSA to provide additional oversight and controls, such as establishing a disaster recovery capability.

- TSA has informed vendors of the need to address systemic cybersecurity issues in future STIP equipment procurement processes.

- TSA's OSC has developed a cybersecurity plan and a cybersecurity management framework for its TSEs. According to OSC officials, the cybersecurity plan is designed to protect OSC's most sensitive and mission critical data and systems and comply with Federal requirements. The cybersecurity management framework outlines a risk-based approach to securing and maintaining OSC's mission-essential functions.

- TSA will perform assessments and determine the operational risk prior to connecting TSEs to the network.

TSA's proposed actions should resolve many of the STIP IT security deficiencies identified in our reports. However, more time is needed to determine the effectiveness of these improvement initiatives. OIG may evaluate the impact of these improvements at a future date.

Appendix A
Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

We previously reported on deficiencies in IT security controls of STIP, a data management system that connects airport screening equipment to a centralized server. We conducted this audit to assess the extent of the deficiencies and the actions TSA has taken to address them. We performed onsite inspections of the areas where STIP servers and switches are located at Orlando International Airport, interviewed departmental staff, reviewed documentation, and observed technical tests of computer security controls for STIP servers.

We coordinated the implementation of this audit of IT security controls with DHS CISO. We interviewed TSA staff. We visited TSA facilities at Orlando International Airport. We compared the DHS IT infrastructure that we observed on site with the documentation provided by the auditees. We observed DHS staff performing vulnerability scans on STIP servers. This activity included TSA staff running their vulnerability detection software against STIP servers and providing OIG with output reports for analysis. The vulnerability scanning software categorizes the vulnerabilities on a scale of 0 to 10. For our analysis, we only reviewed vulnerabilities rated between 7 and 10, inclusive. We consider these 'high' vulnerabilities that should be addressed as soon as possible.

We reviewed Information Assurance Compliance System documentation, such as the authority-to-operate letter, contingency plans, and system security plans. We reviewed guidance DHS provided to its components in the areas of system documentation, information security patch management, and wireless security. We reviewed applicable DHS and component policies and procedures, as well as government-wide guidance. We provided briefings and presentations to TSA staff on the results of our fieldwork and the information summarized in this report.

We conducted this performance audit between May 2015 and December 2015 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require

that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts of DHS management and staff to provide the information and access necessary to accomplish this review. Major OIG contributors to the audit are identified in appendix F.

Appendix B
Agency Comments to the Draft Report

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation Security Administration

APR 0 8 2016

MEMORANDUM FOR: Sondra McCauley
Assistant Inspector General
for Information Technology Audits
U.S. Department of Homeland Security
Office of the Inspector General

FROM: Peter V. Neffenger
Administrator

SUBJECT: Management's Response to OIG Draft Report: "IT Management Challenges Continue in TSA's Security Technology Integrated Program." (Project No. 15-011-ITA-TSA)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

The Security Technology Integrated Program (STIP) is an agency-wide information and technology management program within the Transportation Security Administration (TSA) Office of Security Capabilities that enables TSA to move their established airport security system to the next generation of capability by connecting the myriad of Transportation Security Equipment (TSE) to one network. STIP establishes a centralized enterprise data management system that facilitates the exchange of information between TSE located at the Nation's airports and the people who use, procure, and service them.

The primary challenge is that much of our TSE was fielded before there was the concept that they might be connected on a common Transmission Control Protocol/Internet Protocol (TCP/IP)-based network. Like other unique equipment in service across the government, original TSE development was not created with current cyber security threats in mind. As such, retrofitting these mission-essential tools with up-to-date cybersecurity capabilities designed for current traditional IT systems is extremely challenging and resource intensive.

In light of these challenges, TSA appreciates OIG's acknowledgement of the steps that TSA has taken to resolve cybersecurity deficiencies related to TSE. Specifically, TSA has articulated nine specific cybersecurity requirements that all technology vendors will be required to implement on current and future technologies, which will bring them into compliance with cyber security requirements. However, it's important to note that the implementation of the requirements will be dependent on the cost/schedule proposed by the vendors and the availability of funds to execute the cybersecurity remediation contracts.

The draft report contained eleven (11) recommendations with which the TSA concurs. Specifically:

Recommendation 1: Ensure that IT security controls are included in STIP system design and implementation so that STIP servers are not deployed with known technical vulnerabilities.

Response: Concur, although it is important to note that "STIP servers at airports" should be denoted, in the interest of accuracy, as Multi-Plexor (MUX)/in-line Explosives Detection System (EDS) servers. While STIP System Authority to Operate boundary contains EDS and associated IT equipment within its boundary, the actual acquisition of the EDS is managed by Electronic Baggage Screening Program (EBSP), which is a separate non-IT acquisitions program (DHS Level I).

TSA has developed a Cybersecurity Statement of Objectives (SOO) inclusive of critical requirements to bring legacy TSE – including the EDS servers – into compliance with IT security controls mandated by DHS. Additionally, future procurements must include these requirements. Further, TSA has placed STIP datacenter servers within the boundaries of the Infrastructure Core Services system that contains other TSA servers to improve management of IT security of STIP servers at data centers. TSA has also created a formal Cybersecurity Management Framework and Plan that lays out an organizational framework and strategy to oversee the implementation of IT Security requirements onto legacy TSE. The plan also provides the program management support with the appropriate resources to maintain the new IT Security regime for TSE.

TSA will issue the Cybersecurity SOO to current TSE vendors by the end of August 2016. The implementation of the requirements on the current TSE will be dependent on the cost/schedule proposed by the vendors and TSA's availability of the funds to execute the cybersecurity remediation contracts. TSA has initially estimated that $466M in future year funding is needed to remediate the current fleet of legacy TSE and provide the necessary support and staff to manage the operations and maintenance needed to meet the ongoing cybersecurity requirements. To note, these initial estimates will be refined into a more precise cost estimates as TSA evaluates the vendor proposals in response to the Cybersecurity SOO and begins to implement cybersecurity controls for both STIP and the TSE.

ECD: 8/31/2016 for issuance of Cybersecurity SOO to all vendors.

Recommendation 2: Ensure that STIP servers use approved operating systems for which the Department has established minimum security baseline configuration guidance.

Response: Concur. In April 2015, TSA began efforts to catalogue and disconnect any TSE not running a supported Operating System (OS). Currently, TSA has made progress to replace outdated Windows operating systems and will continue its effort until TSE run on a supported OS. The Cybersecurity SOO contains a requirement around Operating System Currency/Security Patching that will address this recommendation. As stated above, specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts.

TSA has continued to work with vendors to remediate TSE with expired operating systems that cannot be entirely removed from the screening process due to their criticality to mission effectiveness. TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure while outdated OS are phased out of the enterprise. To this end, TSA has initiated comprehensive market research to identify the latest cybersecurity tools that can be applied to the endpoint devices, as well as network infrastructure that will best mitigate cybersecurity risk to the enterprise while allowing connectivity needed for security effectiveness and efficiency. The market research will be completed by the end of May 2016. TSA will then engage with identified vendors to collaborate on Proofs of Concept to validate requirements and capabilities that can transition to an enterprise-wide implementation.

ECD: 5/31/2016 for completion of market research for cybersecurity mitigation tools; 8/31/2016 for issuance of Cybersecurity SOO to all technology vendors.

Recommendation 3: Ensure that STIP servers have the latest software patches installed so that identified vulnerabilities will not be exploited.

Response: Concur. TSA has taken steps to identify and implement IT security controls to position the Agency for future defense against cybersecurity attacks on the TSE. Per response to previous recommendation, the Cybersecurity SOO contains a requirement around Operating System Currency/Security Patching that will address this recommendation. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts. Please note that the specific nature of TSE requires them to be tested for OS patch compatibility before the patches are installed. Such patches can only be completed by the vendors due to the proprietary nature of their systems. Keeping these constraints in mind, TSA is developing a process map to remotely patch TSE.

ECD: 5/31/2016 for completion of market research for cybersecurity mitigation tools; 8/31/2016 for issuance of Cybersecurity SOO to all technology vendors.

Recommendation 4: Ensure that IT security testing is performed so that STIP servers are not deployed with known technical vulnerabilities.

Response: Concur. TSA has already mandated IT Security Scanning by engineers from the TSA Office of Information Technology (OIT) Information Assurance Division (IAD) during Integration Testing of STIP EDS servers and any updated software images. Findings are translated into formal Plan of Actions and Milestones (POA&M) for IT Security remediation and assigned different levels of urgency from critical to low and associated timeframes to correct. Timely POA&M remediation is also one of the key requirements embedded in the TSA Cybersecurity SOO that are being issued to technology vendors.

ECD: 6/30/2016 to change STIP Information Systems Security Officer (ISSO) governance document to mandate IAD scanning of EDS servers during formal Integration Testing events that are STIP-related.

Recommendation 5: Ensure that authorized TSA staff obtain and change administrator passwords for STIP servers at airports so that contractors no longer have full control over this equipment at airports.

Response: Concur. TSA Cybersecurity SOO includes requiring access to the TSE to be adjudicated through the Personal Identity Verification (PIV) card validation system provided and controlled by TSA through the Security Technology Integrated Program (STIP). PIV card holders would also have to successfully undergo a TSA-mandated vetting process in order to be issued a PIV card. This means that everyone – including technology vendor and maintenance contractors – will have been vetted and would have to log into a specific TSE using his/her PIV card. Further, the TSA Cybersecurity SOO mandates that TSA obtain administrative access to conduct remote security scanning of TSE every 72 hours – per DHS mandate – and receive log files in near real-time. This gives TSA full visibility on any activities that are performed on a TSE. TSA cybersecurity requirements, when implemented TSE fleet-wide, will give TSA full control over access to TSE as well as near real-time visibility on any activities performed on TSE. As stated above, specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts. TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure as we explore the potential operational impacts to PIV implementation. To this end, TSA has initiated comprehensive market research to identify the latest cybersecurity tools that can be applied that will best mitigate cybersecurity risk to the enterprise while allowing connectivity needed for security effectiveness and efficiency.

ECD: 6/30/2016 to change STIP ISSO governance document to mandate IAD scanning of EDS servers during formal Integration Testing events that are STIP-related.

Recommendation 6: Implement a contractor oversight process so that only authorized and approved software, along with timely updates, is installed on STIP airport servers.

Response: Concur. In accordance with the TSA Cybersecurity Plan, TSA will review logical and physical access controls as they apply to TSE, including an audit of privileged user access. This effort will also include an analysis of maintenance and development contracts to ensure necessary controls are contractually in place to prevent unauthorized use of these systems. Automated configuration audits will also be possible once TSA Cybersecurity SOO requirements are implemented to identify any unauthorized deviation from approved configuration baseline for TSE. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts.

ECD: 8/31/2016 for issuance of Cybersecurity SOO to all technology vendors.

Recommendation 7: Inventory all locations at Orlando International Airport housing STIP servers and switches and ensure that these locations comply with DHS policy concerning physical security and environmental controls.

Response: Concur. TSA is currently planning an asset inventory effort to identify and validate the locations of TSA-owned IT equipment attached to TSE, including STIP (EDS) servers and associated peripherals. This effort will serve to address the immediate needs of identifying locations and equipment, and will also provide information to be used for improving the asset

management process. The project will include three phases, with a primary focus on airports that contain MUX STIP Servers and peripherals. Once completed, TSA intends to identify areas of focus for additional oversight and asset control. The initial phase will involve the National capital region airports and will conclude by July 31, 2016. Based on the lessons learned from the initial phase, the timeline for an enterprise wide asset inventory effort for TSE-related IT equipment will be established.

ECD: 7/31/2016 for the completion of the first phase of the Asset Discovery Study.

Recommendation 8: Ensure an adequate operational recovery capability for STIP servers at DC1 in case DC2 becomes inaccessible.

Response: Concur. TSA will conduct an analysis to determine the level of effort necessary to create full operational recovery capabilities in an alternate location for the STIP servers presently operating in Data Center 2 (DC2). Data Center 1 (DC1) and the Cloud are an option, but TSA will also look to identify other locations that might prove to be more cost effective while delivering the same recovery capability. The analysis to identify a solution and the level of effort required will be completed by the end of September 30, 2016. The implementation of the solution will be dependent on the availability of funds and acquisition of the engineering services required.

ECD: 9/30/2016 for the completion of the analysis and development of options.

Recommendation 9: Establish a process for providing STIP server vulnerability assessment reports to the Department so that DHS leadership may adequately monitor system compliance capability.

Response: Concur. TSA OIT's IAD already provides vulnerability assessments reports for STIP data center servers. TSA will review for any gaps in this reporting and ensure that vulnerability assessment reports are provided for all applicable STIP servers in the data center. As for STIP EDS servers at airports, the recommendation would require manual scanning for each individual server in their current unconnected state. Aforementioned TSA Cybersecurity SOO mandates that TSA obtain administration access to conduct remote security scanning of TSE every 72 hours to identify any compliance gaps on the TSE. Specific timelines for implementation vary and are dependent on each vendor and TSA's ability to fund those efforts.

ECD: 8/31/2016 for issuance of Cybersecurity SOO to technology vendors.

Recommendation 10: Ensure that IT security requirements are included in equipment procurement contracts for IT components of STIP and passenger and baggage handling systems as required.

Response: Concur. For the TSE, TSA will specify the nine cybersecurity requirements that must be met by various TSE vendors prior to connection to TSANet. These nine cybersecurity requirements aim to prevent future cybersecurity threats from becoming realized attacks and are detailed in the TSA Cybersecurity SOO. They are as follows:

1. OS Currency/Security Patching - TSE OS shall be patched to current OS vendor-supported versions when first delivered. Patches will be updated every 30 days. For critical vulnerabilities, the Original Equipment Manufacturer (OEM) will patch per the prescribed time window as determined on a case by case basis.
2. OS Hardening - TSE shall be compliant with the approved DHS Hardening Guidelines for the platform on which they are being developed.
3. Anti-Virus Updates - TSE shall include TSA-approved anti-virus (AV) software configured to receive digitally signed automatic AV virus definition file updates remotely.
4. Security Scanning Support - In support of TSA's efforts to ensure devices are compliant with IT Security requirements, TSE will be assessed and scanned by the OIT IAD. OEM technicians to be on-site as necessary to provide access to the TSE.
5. Security Operations Center (SOC) Monitoring - TSE endpoints shall be monitored by the TSA SOC. TSE shall include TSA-approved Continuous Diagnostics and Mitigation software configured to enable SOC monitoring.
6. Personal Identity Verification (PIV) Card Authentication Compatibility - Privileged TSE users shall be vetted by TSA's Personnel Security Division and audited by IAD annually. Privileged users shall use PIV cards issued by TSA to access the TSE. Vendors will be required to make their TSE compatible with TSA-issued PIV.
7. Technical Obsolescence - TSE contracts shall include technical obsolescence clauses that mandate the upgrade and/or replacement of any software or hardware components that are considered to be Configuration Items that are no longer actively supported by the manufacturer.
8. POA&M Remediation - Upon completion of security scans, findings will be documented and categorized as high, medium, or low based on their potential impact to the TSE IT Security posture. OEMs will support the remediation of open POA&M items in a timely manner.
9. Vendors Information System Security Officer (ISSO) Designation - If TSA has procured Full-Rate Production TSE from an OEM, the OEM will be required to have a designated ISSO to coordinate with TSA ISSOs on IT Security issues.

While TSA will work closely with vendors to implement these requirements on legacy and future TSE, TSA will also actively investigate and put into place compensating security controls as an interim risk mitigation measure as non-compliant TSE are phased out of the enterprise. The comprehensive market research to identify the latest cybersecurity tools as well as network infrastructure that will best mitigate cybersecurity risk will be completed by the end of May 2016. TSA will then engage with identified vendors to collaborate on Proofs of Concept to validate requirements and capabilities that can transition to an enterprise-wide implementation.

ECD: 5/31/2016 for completion of market research for cybersecurity mitigation tools; 8/31/2016 for issuance of Cybersecurity SOO to all technology vendors.

Recommendation 11: Institute controls so that all IT costs associated with STIP are accurately captured and reported in annual budget submissions as required.

Response: Concur that IT costs should be accurately tracked and reported. However, the current policy framework requires all programs to be designated IT or non-IT. This would mean that the Passenger Screening Program (Non-IT DHS Level I Acquisition Program) and Electronic Baggage Screening Program (Non-IT DHS Level I Acquisition Program), which are the programs responsible for managing the acquisitions of the TSE, would have to be redesignated as IT programs in order to meet this recommendation within the current governance framework. Such program redesignation would impose substantial programmatic and cost burden on PSP and EBSP. It would also impose significant personnel suitability constraints (e.g. citizenship requirement, etc.) on current and future TSE procurement and maintenance contracts that would be disruptive to current security operations and impact TSA's mission readiness.

TSA proposes creating an alternate program designation for PSP and EBSP that have both IT and non-IT elements. The handling of these "hybrid" or "mixed" programs will require program-specific tailoring of governance that take into account the oversight and reporting requirements of DHS (Program Accountability and Risk Management, Developmental Test and Evaluation, and Chief Information Officer) and TSA (Chief Information Officer, Chief Technology Officer, Component Acquisition Executive, and Chief Financial Officer). Through this tailoring process, TSA will investigate how costs for TSE can best be captured into IT and non-IT components to be reported accordingly to inform the cost reporting, budget submissions, as well as the Capital Planning Investment Control process. To note, Customs and Border Patrol has recently instituted a tailored governance process for "mixed" programs for similar systems that TSA will benchmark to adapt to its own use for TSE acquisition programs. By the end of April 2016, TSA will establish a working group consisting of the aforementioned stakeholder groups to examine the governance tailoring options and submit recommendations to the DHS and TSA leadership by the end of fiscal year 2016.

ECD: 4/30/2016 for the formal establishment of a working group to develop recommendations on how to best tailor governance for mixed programs; 9/30/2016 for presentation of options to senior leadership.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Appendix C
Designation of IT versus Non-IT Programs

U.S. Department of Homeland Security Arlington, VA 22202

Transportation Security Administration

MEMORANDUM FOR: Carol DiBattiste
Deputy Administrator, TSA

FROM: Tom Blank
Associate Administrator/
Chief Support Systems Officer

SUBJECT: Determining IT versus Non-IT Programs

Our recent TSA IRB proceedings highlight the need to clarify policy and procedures for designating TSA investments as information technology (IT) programs and non-IT programs.

I have reviewed the three key directives associated with this issue – DHS MD 1400, the Clinger-Cohen Act, and OMB Circular A-11, as well as pertinent sections under United States Code. After reviewing this information with an eye toward TSA organization and best business practices, I've made the following determinations:

1) For purposes of Exhibit 300 submissions, a program is an IT program only when the preponderance of the effort is related to information technology. I find that designating programs as "IT" unnecessarily adds significant workload for Program Managers.

2) Programs determined to be IT programs must be under the full purview of the OCIO, including all budget.

3) As almost all non-IT programs have an IT component to them, the IT component of those programs must be under the full purview of the OCIO. In these cases, the OCIO essentially delivers the IT solution to the broader program.

4) The OCIO is the sole executive agent and Participating Manager (PARM) for all IT elements or aspects of TSA investments or programs. As such, the OCIO shall have full visibility and access to acquisition planning and program requirements generation early in the planning process. Regardless of the IT designation of a program, management responsibility, including funds control and project oversight for IT components, should be under the control of OCIO.

- 1 -

5) The TSA CPE is the sole executive agent for TSA program management. As such, the CPE is responsible for all aspects of the program management discipline within TSA, including oversight for program requirements generation, acquisition planning, review, reporting, and execution.

6) Notwithstanding full IT visibility and oversight within TSA, the TSA OCIO shall develop and adopt procedures that designate individual programs as IT programs, when the preponderance of the effort is related to Information Technology, primarily adhering to definitions contained for information systems per US Code section 1401 of Title 40.

7) As part of my findings, and to resolve relevant action items from recent TSA IRB proceedings, I will direct the TSA CPE and OCIO to re-designate programs as follows:

- The TSA HR Services program (Sections I and II), because it is essentially a service contract, shall be designated as a non-IT program.
- The TSA Passenger Screening Program (Aviation) shall be designated as a non-IT program.
- The proposed integration program for Electronic Baggage Screening and Passenger Screening (known as CASSNET), if approved, shall be designated as an IT program.

8) I will further direct that all IT components of these programs will be under the control of the OCIO.

cc: Chief Operating Officer (TSA)
Chief Information Officer (TSA)
Chief Financial Officer (TSA)
Chief Procurement Executive (TSA)

Appendix D
Data Center and Airport STIP Server Vulnerabilities[6]

STIP Server Name	Total Number of High Vulnerabilities Related to [redacted]	Additional High Vulnerabilities[8]	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
[redacted]	593	1	No
	395	2	Yes
	395	4	Yes
	541	1	Yes
	541	2	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes
	-	1	Yes

[6] The scanning software used for this audit scores vulnerabilities on a scale of 0 to 10, which is based on the Forum of Incident Response and Security Teams' Common Vulnerability Scoring System. Within this system, the more easily a vulnerability can be exploited, the higher the vulnerability score. For this report, vulnerabilities scored over 6.9 are considered to be 'high.'
[7] A total of 9,263 high server vulnerabilities were associated with only two software applications [redacted]
[8] The technical scans also detected an additional 3,019 high vulnerabilities that were not related to [redacted]

STIP Server Name	Total Number of High Vulnerabilities Related to [redacted]	Additional High Vulnerabilities	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
[redacted]	-	1	Yes
	-	1	Yes
	-	2	Yes
	-	1	Yes
	1	4	Yes
	1	4	Yes
	1	4	Yes
	1	4	Yes
	-	99	No
	-	99	No
	-	99	No
	-	99	No
	-	99	No
	-	127	No
	-	99	No
	-	99	No
	1025	84	Yes

STIP Server Name	Total Number of High Vulnerabilities Related to [redacted]	Additional High Vulnerabilities	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
[redacted]	1012	41	Yes
	758	96	Yes
	395	5	Yes
	571	5	Yes
	609	5	Yes
	550	376	Yes
	541	11	Yes
	-	5	Yes
	-	5	Yes
	-	5	Yes
	-	5	Yes
	-	5	Yes
	266	142	No
	265	35	No
	266	143	No
	266	143	No
	266	143	No
	-	6	No
	-	6	No
	-	6	No

STIP Server Name	Total Number of High Vulnerabilities Related to Adobe Systems or Oracle's Java	Additional High Vulnerabilities	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
[redacted]	-	6	No
	-	6	No
	-	38	No
	-	6	No
	-	6	No
	-	6	No
	-	6	No
	1	3	No
	1	3	No
	1	35	No
	1	35	No
	-	-	Yes
	-	-	Yes
	-	-	Yes
	-	89	No

STIP Server Name	Total Number of High Vulnerabilities Related to [redacted]	Additional High Vulnerabilities	Vulnerability Assessments Provided to the DHS Vulnerability Management Branch?
[redacted]	-	89	No
[redacted]	-	93	No
[redacted]		93	No
[redacted]		93	No
[redacted]		93	No
[redacted]		93	No
[redacted]		93	No
Totals of 74 Servers:	9,263	3,019	

Source: OIG-compiled based on data from TSA testing results.

Appendix E
Office of IT Audits Contributors to This Report

Sharon Huiswoud, IT Audit Director
Kevin Burke, Supervisory IT Auditor
Charles Twitty, Senior IT Auditor
Robert Durst, Senior Program Analyst
Anna Hamlin, Referencer

Appendix F
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Director, Government Accountability Office/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
DHS CISO
DHS CISO Audit Liaison
Administrator, TSA
Assistant Administrator for Office of Security Capabilities, TSA
TSA CIO
TSA Audit Liaison
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305