Department of Homeland Security

Office of Inspector General

Transportation Security Administration Information Technology Management Progress and Challenges

OIG-13-101

June 2013

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 24, 2013

MEMORANDUM FOR: John W. Halinski
Deputy Administrator
Transportation Security Administration

FROM: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Transportation Security Administration Information Technology Management Progress and Challenges*

Attached for your action is our final report, *Transportation Security Administration Information Technology Management Progress and Challenges.* We incorporated the formal comments from the Transportation Security Administration (TSA).

The report contains five recommendations aimed at improving TSA's information technology management. Your office concurred with 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) corrective action plan and (2) 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. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security.

Please call me with any questions, or your staff may contact Richard Harsche, Division Director, Information Technology Audits, at (202) 254-5448.

Attachment

Table of Contents

Appendixes

Abbreviations

AIT	Advanced Imaging Technology
CIO	Chief Information Officer
DHS	Department of Homeland Security
EDS	Explosives Detection System
eTAS	Electronic Time, Attendance, and Scheduling
FAMS	Federal Air Marshal Service
FY	fiscal year
GAO	Government Accountability Office

IT	information technology
ITAR	Information Technology Acquisition Review
MD	Management Directive
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
SELC	systems engineering life cycle
TSA	Transportation Security Administration

Executive Summary

Information technology plays a critical role in enabling the Transportation Security Administration (TSA) to accomplish its mission. In 2007, we reported that TSA did not manage and apply information technology effectively to support accomplishment of its mission objectives. We conducted a follow-up audit to determine TSA's progress in establishing key information technology management capabilities to support mission needs. Appendix A describes the audit's scope and methodology.

The TSA Chief Information Officer has established key information technology management capabilities to support TSA's mission. Specifically, the Chief Information Officer updated the information technology strategic plan, implemented a systems engineering life cycle process to manage information technology programs, implemented information technology acquisition review processes, and developed an enterprise architecture. Not all information technology procurements, however, have gone through the information technology acquisition review process because they were not categorized as information technology procurements. As a result, there is little assurance that all information technology investments are aligned with the Chief Information Officer's strategy or TSA's future information technology mission needs.

The TSA Chief Information Officer faces challenges in ensuring that the information technology environment fully supports TSA's mission needs. Specifically, TSA's information technology systems do not provide the full functionality needed to support its mission due to challenges with TSA's requirements gathering process. As a result, staff created manual workarounds or developed local systems to accomplish their mission. In addition, information technology support roles are not well defined or communicated, and the number of information technology support staff is not sufficient at certain field sites. Some field sites detailed employees from operational areas to fill in gaps in information technology support, which reduced the number of staff available to serve at security checkpoints and may hinder TSA's ability to carry out its mission.

We made five recommendations to the Deputy Administrator, Transportation Security Administration, to ensure that the Department's definition of information technology is applied for all acquisitions; develop and implement a process to ensure that all information technology acquisitions go through information technology acquisition review; develop and implement a process to capture information technology requirements in the field; communicate the IT specialist role, as contractually defined, to both IT specialists and to the user community; and develop and implement a process to provide sufficient IT support in airports and operational sites in the field.

Background

TSA was created in the wake of September 11, 2001, to maintain the security of transportation systems and the traveling public. By the end of 2002, TSA had deployed a security operations workforce and assumed 100 percent of all airport screening responsibilities. Originally part of the Department of Transportation, transportation security functions moved to the Department of Homeland Security (DHS) in March 2003.

TSA's mission is to strengthen the security of the Nation's transportation systems while ensuring the freedom of movement for people and commerce. To accomplish its mission, TSA's nearly 50,000 Transportation Security Officers screen more than 1.7 million passengers each day at more than 450 airports nationwide. TSA uses approximately 2,800 Behavior Detection Officers at airports across the country, and thousands of Federal Air Marshals are deployed every day on domestic and international flights. TSA has more than 400 explosives specialists in aviation and other transportation environments. To date, TSA has deployed more than 800 Advanced Imaging Technology machines at airports, leading to the detection of prohibited, illegal, or dangerous items. In fiscal year (FY) 2013, TSA's budget was approximately $7.6 billion, which represents 13 percent of DHS' overall budget of approximately $59 billion.

Information technology (IT) systems play a critical role in enabling TSA to accomplish its mission. TSA's Office of Information Technology (OIT) is responsible for developing and managing IT initiatives and policies for TSA's IT requirements. OIT supports approximately 70,000 government and contractor personnel, working at more than 450 airports and at 22 international locations, who use approximately 33,000 computers, 26,000 phones, 4,000 switches, 750 routers, and 90,000 email accounts. As of October 2012, OIT employed 1,957 staff, including 230 Federal employees and 1,727 contractors. In FY 2013, TSA requested an IT budget of approximately $417.2 million.

To plan and manage TSA's critical IT environment, OIT is organized into five offices: the Senior Technical Advisor and DHS Liaison Office, the Business Management Office, Federal Air Marshal Service (FAMS) IT, IT Strategy and Innovation, and IT Operations, as shown in figure 1.

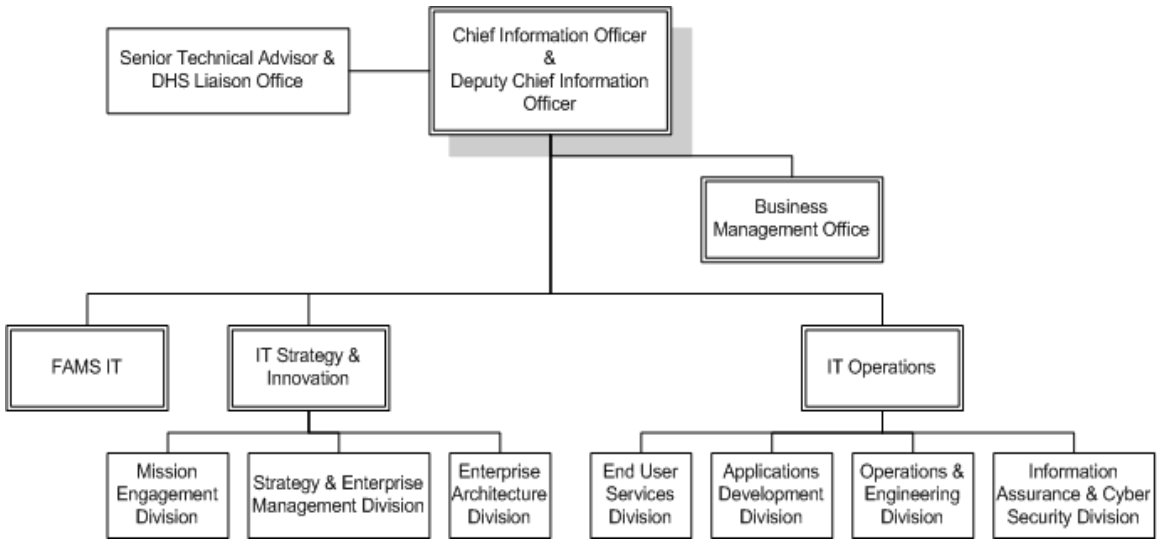

Figure 1. TSA's OIT Organizational Structure as of June 2012

The Senior Technical Advisor and DHS Liaison Office is responsible for defining the next generation of TSA and DHS target IT capabilities, based on mission needs. The Business Management Office ensures that IT is appropriately aligned with OIT, TSA, and DHS goals and priorities. FAMS IT manages service-wide planning, development, acquisition, testing, integration, installation, security, use, and evaluation of its IT systems, facilities, services, and procedures.

IT Strategy and Innovation provides strategic and enterprise services in support of TSA's IT programs. Within IT Strategy and Innovation, the Mission Engagement Division builds and strengthens customer-partner relationships between OIT and TSA mission and support offices. The Strategy and Enterprise Management Division maintains the TSA IT strategic plan, creates the OIT annual report, and develops the IT roadmap strategy from the current, as-is to the future, to-be TSA enterprise environment. Finally, the Enterprise Architecture Division provides vision and expertise in enterprise architecture and enterprise data management services.[1]

IT Operations provides IT support to more than 70,000 users across the agency and manages IT projects. IT Operations is responsible for 24x7 operations centers, including the Security Operations Center, Network Operations Center, and Help Desk Services. Within IT Operations, the End User Services Division provides office automation

[1] Enterprise architecture is a management practice designed to maximize the contribution of an agency's resources, IT investments, and system development activities to achieve mission performance goals.

services, desk side support, and customer-focused IT project management to more than 3,000 users. This division also serves as the primary customer interface for IT products and services for more than 120 Federal Security Directors and their more than 50,000 staff at domestic and international locations. Also under IT Operations, the Applications Development Division provides enterprise-wide software solutions, and the Operations and Engineering Division provides project engineering services for all new IT services. Finally, the Information Assurance and Cyber Security Division coordinates audits on TSA internal systems, TSA contractor-managed systems, and airports, and is responsible for the communications and outreach activities related to cyber security for the agency.

OIT is responsible for developing and implementing enterprise-wide common applications and systems resulting in efficient, cost-effective, secure, and interoperable solutions to customer requirements. OIT manages some systems, but other TSA offices outside of OIT, including the Office of Security Capabilities and the Office of Intelligence and Analysis, manage other systems. TSA's major systems include the following:

Major Systems Managed by OIT

- Information Technology Infrastructure Program – This program provides a communication and data processing platform that is used by all headquarters and TSA field elements to perform their mission of providing transportation security. The program includes email; database support; personal device communications; software and hardware refreshment; and hotline, technical, and security support.
- Performance Management Information System – This system is an enterprise-level analytical tool that integrates data from multiple sources to collect and report on a variety of TSA performance measures in order to monitor TSA's progress toward operational goals.
- TSA Operating Platform – This platform is a collection of shared IT components and services that support mission critical applications across TSA. The platform enables a streamlined provisioning process to acquire secure and reliable information and applications to meet legislative mandates and deliver integrated database and network resources.
- FAMS Mission Scheduling and Notification System – This system is the technology interface between FAMS and the airline industry and provides a variety of scheduling tools to help FAMS execute its mission.

Major System Managed by the Office of Security Capabilities

- Security Technology Integrated Program – This program is an agency-wide data management system that provides a centralized focal point connecting

passenger and baggage screening security technologies to one network to address data, threat response, and equipment challenges.

Major Systems Managed by the Office of Intelligence and Analysis

- Secure Flight – Secure Flight is a behind-the-scenes program that enhances the security of domestic and international commercial air travel through the use of improved watch list matching.
- Technology Infrastructure Modernization Program – The purpose of this program is to provide a robust and integrated enrollment, vetting, and credentialing system capable of providing services to TSA while meeting the anticipated rate of growth of the transportation worker population.

Effective management of IT systems is important to ensure that mission operations are supported. Previous audits have identified challenges with TSA's IT infrastructure and management. For example, in 2007, we reported that TSA's IT infrastructure had limited system integration and data sharing and had perpetuated inefficient manual work processes.[2] Additionally, because of limitations with authority and a need for standard IT governance policies across TSA, the agency's Chief Information Officer (CIO) faced significant challenges in conducting agency-wide IT planning and investment management. Insufficient OIT staff also impeded the CIO's ability to manage the IT infrastructure and support new technology requirements.

To address those challenges, we recommended that the Assistant Administrator for TSA strengthen component IT management by empowering the CIO with agency-wide IT budget and investment review authority; develop a consolidated strategic planning approach; complete and implement an enterprise architecture; establish and communicate guidelines and procedures for acquiring, developing, and managing IT solutions in a consistent, integrated, and efficient manner; and apply adequate staff resources to address IT needs and provide support to TSA operations agency-wide. In response, TSA advised the DHS Office of the Inspector General (OIG) that it had updated the IT strategic plan, developed an enterprise architecture system and repository, revised its investment review process, and conducted an analysis of its organizational structure and staff. Based on TSA's actions, we closed the five recommendations. As part of this audit, we revisited these areas to determine TSA's progress in establishing key IT management capabilities to support mission needs.

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

Results of Audit

IT Management Capabilities Established

The CIO has taken actions to establish key IT management capabilities to support TSA's mission. Specifically, the CIO updated its IT strategic plan to guide OIT in supporting TSA and Department mission goals. In addition, the CIO implemented a systems engineering life cycle (SELC) process to manage IT programs. The CIO also implemented IT Acquisition Review (ITAR) processes and developed an enterprise architecture. These actions can help support effective IT management and ensure that IT investments provide effective support for TSA's transportation security mission.

Strategic Planning

The *Government Performance and Results Act of 1993* holds Federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results.[3] Additionally, Office of Management and Budget (OMB) Circular A-130, as revised, instructs agency CIOs to create strategic plans that demonstrate how information resources will be used to improve the productivity, efficiency, and effectiveness of government programs.[4] DHS Management Directive (MD) 0007.1 requires component CIOs to develop and implement an IT strategic plan that clearly defines how IT supports an agency's mission and drives investment decisions, guiding the agency toward its goals and priorities.[5]

The TSA CIO has an up-to-date strategic plan that is in line with Federal requirements and Department guidance. Specifically, the CIO developed the *TSA IT Strategic Plan, FY 2012–2016* in October 2011. The plan identifies an actionable and measurable IT strategy that articulates the CIO's vision, mission, goals, and objectives through FY 2016. Table 1 shows the five goals included in the plan.

[3] Public Law 103-62, *Government Performance and Results Act of 1993*, August 3, 1993.
[4] OMB Circular A-130, *Management of Federal Information Resources*, Transmittal Memorandum #4, November 28, 2000.
[5] DHS MD 0007.1, *Information Technology Integration and Management*, March 15, 2007.

Table 1. TSA OIT Strategic Goals

TSA OIT FY 2012-16 Strategic Goals
Goal 1: Deliver IT services that are aligned to TSA's mission and business needs through collaboration and implementation of best practices
Goal 2: Provide an information environment that fosters secure collaborative information sharing among TSA and its stakeholder organizations
Goal 3: Evolve the IT infrastructure into a cohesive architecture to optimize service delivery
Goal 4: Strengthen the cyber security and information assurance capability to ensure TSA assets and operations are protected
Goal 5: Develop and implement a comprehensive approach to ensure excellence of IT delivery through recruitment, development, retention, and recognition

To accomplish these goals, the TSA CIO has established specific objectives with associated key performance metrics. For example, to meet the goal to develop and implement a comprehensive approach to ensure excellence of IT delivery through recruitment, development, retention, and recognition, the plan identifies two objectives—to provide comprehensive and effective IT human capital management, and to establish a career path framework aligned with IT competencies that support succession management. For each of these objectives, the plan defines key performance metrics that will measure progress toward achieving the goal. For example, the implementation of an integrated TSA IT human capital plan and the development of a career path framework for IT learning and development will contribute to TSA OIT's goal to develop an approach to ensure excellence of IT delivery.

The *TSA IT Strategic Plan, FY 2012–2016* aligns with the goals identified in the DHS and TSA strategic plans. The plan is also aligned with the *DHS IT Strategic Plan 2011–2015* to ensure that TSA OIT supports the DHS CIO's department-wide IT goals. Table 2 shows the alignment of OIT goals with DHS and TSA goals.

Table 2. Alignment of TSA OIT Goals with TSA, DHS, and DHS IT Goals

Alignment of TSA OIT Goals with TSA, DHS, and DHS IT Goals						
TSA OIT		Goal 1	Goal 2	Goal 3	Goal 4	Goal 5
TSA	Goal 1: Risk-based security	✓	✓		✓	
	Goal 2: Workforce engagement	✓				✓
	Goal 3: Organizational efficiency	✓		✓		
DHS	Goal 1: Prevent terrorism and enhance security	✓	✓		✓	
	Goal 2: Secure and manage United States borders	✓	✓			
	Goal 3: Enforce and administer immigration laws	✓				
	Goal 4: Safeguard and secure cyberspace	✓		✓	✓	
	Goal 5: Ensure resilience to disasters	✓	✓	✓		
DHS IT	Goal 1: Establish secure IT services and capabilities to protect the homeland and enhance our Nation's preparedness, mitigation, and recovery capabilities	✓				
	Goal 2: Improve secure and trusted internal and external information sharing	✓	✓		✓	
	Goal 3: Improve transparency, accountability, and efficiencies of services and programs through effective governance and enterprise architecture	✓		✓		
	Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention, and recognition to ensure excellence in IT delivery across the Department	✓				✓

The TSA CIO's development of a well-aligned, up-to-date strategic plan that defines a clear vision and direction positions TSA OIT to provide effective support for TSA's transportation security mission.

Systems Engineering Life Cycle

DHS Acquisition Instruction/Guidebook #102-01-001, Appendix B, requires agencies to follow a SELC process.[6] The purpose of the DHS SELC is to establish a standard system life cycle framework across DHS agencies and to ensure that DHS IT capabilities are delivered efficiently and effectively.

The TSA CIO implemented the DHS SELC process in compliance with departmental guidance. OIT maintains an online site to guide TSA project

[6] DHS Acquisition Instruction/Guidebook #102-01-001, Appendix B, Interim Version 2.0, September 21, 2010.

managers and participants in complying with the DHS SELC. This online tool enables users to tailor the SELC to meet their project needs and contains templates and guidance to aid users in the development of documents for each of the nine stages of the SELC. Figure 2 shows the nine stages of the SELC.

STAGE A Solution Engineering	STAGE 1 Planning	STAGE 2 Requirements Definition	STAGE 3 Design	STAGE 4 Development	STAGE 5 Integration & Test	STAGE 6 Implementation	STAGE 7 Operations & Maintenance	STAGE 8 Disposition
Engineer the program solution to ensure all alternatives are considered	Plan the project and acquire resources needed to achieve solution	Analyze user needs and document functional requirements	Transform requirements into detailed system design	Convert the design into system	Integrate and test with other systems; conduct user acceptance testing; develop Certification & Accreditation	System moved to Production environment; Production data has been loaded	The system is operated to carry out intended function	The system is disposed

Figure 2. TSA SELC Phases

TSA staff initiate the SELC process by submitting a project request to OIT. An OIT Customer Relations Manager works with the staff to match their business requirements with existing IT products and services and to initiate project requests by completing a project authorization document.

The OIT Business Technology Council reviews projects to ensure that all IT projects align to the TSA strategic plan, TSA initiatives and goals, and TSA's enterprise architecture. The OIT General Managers for the IT Strategy and Innovation Office and the IT Operations Office co-chair the council, which meets biweekly, and office division directors serve as members. After the council approves a project, OIT assigns a project manager, who guides staff through the next steps, including defining requirements and creating required SELC documents. For example, a Mission Needs Statement, which states why the investment needs to be undertaken, is required for all IT projects.

The CIO's implementation of the SELC process should help TSA ensure that its IT investments will support TSA and DHS strategic goals.

IT Acquisition Review

DHS MD 0007.1 requires IT acquisitions valued at $2.5 million or greater to be submitted to the DHS CIO for review. This directive also requires component CIOs to implement an ITAR process for IT acquisitions below $2.5 million. ITAR is required before the award of an IT procurement so that acquisitions are aligned with IT policy, standards, objectives, and goals across DHS.

The TSA CIO has implemented an ITAR process that aligns with DHS policies.[7] TSA customers begin the ITAR process by submitting a complete procurement request package with supporting documentation, such as a statement of work, an independent government cost estimate, and market research, to the ITAR "TSAITBUY" team. The ITAR TSAITBUY team sends complete procurement request packages to the appropriate review groups to ensure that the packages comply with TSA acquisition guidelines. Specifically, each IT procurement package must go through enterprise architecture, accessibility, investment level, infrastructure, information security, and records management reviews. For example, the enterprise architecture group determines if the request is part of a program that has been reviewed by the enterprise architecture board, if the customer has submitted a list of hardware and software products included in the request, if the requested products are listed in the Department's approved technology list, and if the request is part of an upgrade to an enterprise service, among other items. The information security group determines, for example, if there are requests for hardware or software that will hold or handle DHS sensitive information, and if so, if the package includes a clause that indicates the request will meet specific security certifications and compliance standards.

Once a procurement request has been approved, requests totaling $2.5 million or more are submitted to the DHS ITAR team for review with subsequent approval by the DHS CIO. The TSA CIO approves requests for less than $2.5 million. In FY 2012, 74 requests were submitted to the DHS CIO, and 698 requests were submitted through the TSA ITAR process.

Enterprise Architecture

The *Clinger-Cohen Act of 1996*, as amended, and OMB circulars mandate the establishment and use of an enterprise architecture to guide and direct government investments from inception through retirement.[8] [9] In addition, OMB Memorandum M-11-29 states that CIOs must use an enterprise architecture to consolidate duplicative investments and applications.[10] An

[7] TSA Management Directive 300.15, *Information Technology Acquisition Review*, signed January 6, 2012, provides TSA policy and procedures for the ITAR process.
[8] Public Law No. 104-106, Division E, February 10, 1996. The law, initially titled the *Information Technology Management Reform Act of 1996*, was subsequently renamed the *Clinger-Cohen Act of 1996* in Public Law No. 104-208, September 30, 1996.
[9] OMB Circular A-130, Revised, *Management of Federal Information Resources*, November 28, 2000; and OMB Circular A-11, Revised, *Preparation, Submission, and Execution of the Budget*, August 3, 2012.
[10] OMB M-11-29, *Chief Information Officer Authorities*, August 8, 2011.

enterprise architecture describes the current architecture, target architecture, and transition strategy for attaining the target goals and objectives. An enterprise architecture enables leadership to prioritize available resources to support mission functions, ensures that mission requirements drive technology investments, and identifies current capabilities and performance gaps and projected future gaps.

The TSA CIO developed an enterprise architecture to align with the Department's architecture and guide TSA's IT environment. From 2011 through 2012, TSA provided the Department with a self-assessment status report each quarter on its enterprise architecture program. In this report, TSA rated its progress against the Government Accountability Office (GAO) Enterprise Architecture Management Maturity Framework.[11] In March 2011, TSA identified its enterprise architecture maturity at stage zero of the six stages of the GAO Enterprise Architecture Management Maturity Framework, meaning TSA was creating enterprise architecture awareness. In its last FY 2012 status report, TSA rated its progress at stage four maturity, which means that TSA has developed an approved version of its enterprise architecture that is used for targeted results, such as guiding investment decisions.

In FY 2012, the Homeland Security Systems Engineering and Development Institute, the Department's federally funded research and development center, began conducting independent, objective reviews of the quarterly status reports of select DHS components. Since the last quarter of FY 2011, TSA had each of its self-assessed enterprise architecture maturity scores independently reviewed and evaluated. As of the last quarter of FY 2012, the institute independently identified TSA's enterprise architecture program at stage four maturity. Figure 3 shows TSA's enterprise architecture maturity within the stages of the Enterprise Architecture Management Maturity Framework.

[11] GAO-10-846G, *A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, August 2010.

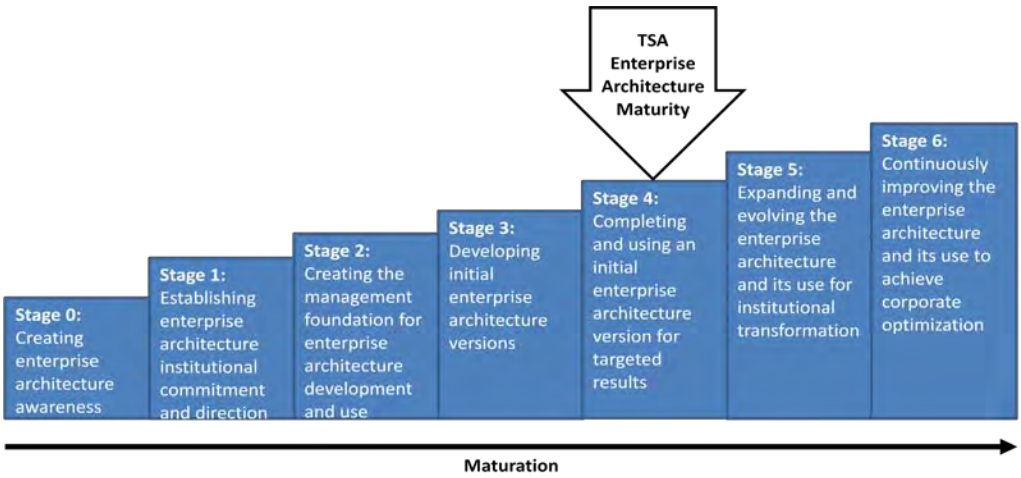

Figure 3. Stages of Enterprise Architecture Management Maturity Framework with TSA Enterprise Architecture Maturity

ITAR Process Implementation Limited

Although the TSA CIO implemented an ITAR process, not all IT procurements have gone through the process. For example, the Explosives Detection System (EDS) and the Advanced Imaging Technology (AIT) procurements did not go through the ITAR process. These systems did not go through the review processes because the responsible program managers did not categorize them as IT procurements. As a result, there was little assurance that all IT investments were aligned with the CIO's strategy or TSA's future IT mission needs. Limited ITAR implementation also hinders the CIO's ability to manage TSA's IT environment, which increases the risk of security issues and hampers cost-saving efforts.

Explosives Detection Systems

EDS units capture images and scan checked baggage to analyze the contents and determine whether explosive threats might be present. In 2009, TSA procured 77 EDS units as part of a contract amounting to approximately $29.9 million. As of October 2010, TSA had 2,297 EDS machines, 1,938 of which were deployed at airports in the United States. EDS units contain IT hardware and software components that display, process, and transmit data.

Advanced Imaging Technology

AIT is used to screen passengers to detect weapons, explosives, and other threats to protect the traveling public. TSA uses two types of AIT, millimeter

wave imaging technology and backscatter technology, to screen passengers for both metallic and non-metallic threats. Both types of AIT units contain IT hardware and software components that display, process, and transmit data. Millimeter wave imaging technology detects threats by displaying a generic outline of a person on a monitor attached to the unit highlighting any areas that may require additional screening. If no anomalies are detected, an "OK" appears on the screen with no outline. Backscatter technology projects an X-ray beam over the body surface and creates an image, transmits this image to a remote location, and displays it on a monitor for a TSA officer to review. The technology has a privacy filter that blurs the image so that it resembles a chalk etching. As of December 2012, there were more than 800 imaging technology devices at approximately 200 airports, and TSA had spent approximately $140 million on AIT equipment.

These IT systems and equipment did not go through the ITAR or enterprise architecture review processes because TSA did not designate all procurements with IT components as IT procurements. Program offices can bypass the ITAR process by identifying a procurement as non-IT. According to TSA's acquisition review process procedures, the program official making the procurement request determines if any of the proposed procurement requirements contain IT components.[12] If the program official determines that the procurement does n ot contain IT, the procurement may not be submitted for ITAR review to ensure that it meets enterprise architecture, application architecture, software management, and security and accessibility requirements.

The Federal Government, DHS, and TSA all have defined IT to include IT equipment or systems that display, manipulate, or transmit data.[13] Although TSA guidance is aligned with the Department's and Federal guidance on the definition of IT, the TSA CIO has authority only over programs that TSA program managers have defined as IT. Even though security technology equipment, such as EDS and AIT, display, manipulate, and transmit data, TSA designated as IT only the portion of the EDS and AIT technologies that connects to the TSA network.

Several TSA officials with whom we met told us that designating programs as "IT" created significant workload for program managers. IT procurements must go

[12] *TSA OIT Acquisition Review Process Standard Operating Procedure*, January 6, 2009, and TSA Management Directive 300.15, *Information Technology Acquisition Review*, signed January 6, 2012.
[13] The Federal, Department, and TSA definitions of IT are shown in appendix C.

through more reviews than those designated as non-IT procurements; therefore, IT procurements typically take longer to go through the acquisition process.

However, the ITAR process enables the CIO to align IT acquisitions with TSA IT policies, standards, objectives, and goals. ITAR also helps the CIO validate TSA's alignment with the DHS enterprise architecture and ensure compliance with security and accessibility requirements. Information Assurance and Cyber Security Division staff have had to modify contracts to include appropriate security language and clauses because these security technologies did not undergo the standard ITAR process. IT acquisitions that do not go through the ITAR process are not subject to alignment reviews and may increase costs for operations and maintenance, limit opportunities for system integration, and create a risk to TSA's IT environment.

Recommendations

We recommend that the Deputy Administrator, Transportation Security Administration:

Recommendation #1:

Direct all TSA program offices to apply the Department's definition of IT for all acquisitions.

Recommendation #2:

Develop and implement a process to ensure that all IT acquisitions, including passenger and baggage screening equipment, go through IT Acquisition Review and receive enterprise architecture, security, and privacy reviews.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Administrator, Transportation Security Administration. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Administrator concurred with our recommendations and provided details on steps being taken to address specific findings and

recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues outlined in the comments below.

In response to recommendation one, the Administrator concurred and stated that TSA has codified the definition of IT in *TSA Management Directive 300.15, Information Technology Acquisition Review*. Further, the Administrator stated that there should be a mechanism for determining the application of the definition of IT in program designations. To adjudicate the application of the definition of IT in program designation, TSA included a process in its draft *Management Directive 1400.20, IT Governance*. That approval process involves the CIO, the Chief Procurement Officer Executive/Component Acquisition Executive, and the Program Office in the IT designation process. We recognize the inclusion of the process in the draft Management Directive 1400.20 as a positive step toward addressing this recommendation, and look forward to learning more about continued progress. This recommendation will remain open pending evidence of further progress in this regard.

In response to recommendation two, the Administrator concurred and stated that IT acquisitions, when determined to be designated as IT, will follow the DHS ITAR guidelines and process. However, the Administrator stated that TSA takes exception to the presumption that the Electronic Baggage Screening Program and Passenger Screening Program are IT programs. We disagree with this assertion. As stated in our report, baggage and passenger security screening equipment displays, manipulates, and transmits data, which meets the Federal definition to be designated as information technology. Although we are encouraged by TSA's actions to establish a process as described in recommendation one to evaluate the program for IT designation, we expect this evaluation to include all IT acquisitions, including security screening equipment. This recommendation will remain open pending evidence of further progress in this regard.

Support of Mission Needs

The TSA CIO faces challenges in ensuring that the IT environment fully supports TSA's mission needs. Specifically, TSA's IT systems do not provide the full functionality needed to support its mission. For example, some systems did not provide the reporting functions needed, and other systems were not compatible or were not integrated. The limited IT functionality experienced in the field is due to challenges with TSA's requirements gathering process. As a result, staff created manual workarounds or developed local systems to accomplish their mission. In addition, IT specialist roles were not well defined or communicated, and the number of IT support staff was not sufficient to support users at certain field sites. Some field sites detailed employees from operational areas to fill in gaps in IT support, reducing the number of staff available to serve at security checkpoints.

IT Functionality

DHS MD 0007.1 states that the component CIO is responsible for timely delivery of mission IT services in direct support of component mission, goals, objectives, and programs. In addition, agencies are required to acquire, manage, and use IT to improve mission performance.[14]

TSA's IT systems do not fully provide the functionality needed to support its mission. Specifically, personnel with whom we spoke identified the following instances in which the systems they used were not sufficient to meet their needs:

- The Electronic Time, Attendance, and Scheduling (eTAS) system that TSA provided for scheduling did not help staff effectively plan for and schedule the numbers and types of staff needed to screen passengers and baggage. Being able to schedule resources efficiently at an airport is important because of the varying amounts of passenger traffic throughout the year and TSA's specific requirements regarding the types of security officers needed at security gates. For example, managers at one airport must schedule 1,300 employees at 22 work locations and ensure that the employees at each checkpoint meet appropriate ratios for gender, part-time staff, and full-time staff. In addition, managers

[14] Public Law 104-13, *Paperwork Reduction Act of 1995*, May 22, 1995.

need to adjust schedules based on peaks in airport traffic, such as holidays. According to users, eTAS reports did not include the necessary data and were not timely. In addition, eTAS was not interoperable with other systems. Users at one site reported that data did not transfer properly between eTAS and an enterprise timekeeping system. Staff had to be taken off of security checkpoints to adjust manually for the differences between the two systems in the number of hours staff worked. Staff at some sites reported that there was no scheduling system with the ability to provide real-time information, such as an employee headcount, and that they had to manipulate three reports generated by enterprise-wide systems in order to obtain necessary operational information such as the hours worked by an employee.

- Users at some airports relied on a business tool that allowed personnel to generate timely, thorough performance measures, metrics, and operational reports, which TSA uses to track and analyze operational data. However, this tool was not compatible with the operating system on the new computers installed as part of the computer replacement program. The staff at these locations switched back and forth between an older operating system to use the reporting tool and the newer operating system for other activities. The Office of Security Operations told us that it had purchased a newer version of the tool that is compatible with the new computers, but this new tool had not been installed at the time of our fieldwork.

- Reports generated from the TSA system for payroll management did not contain up-to-date information. Personnel at one airport stated that it could take 2 to 4 weeks for a new hire to show up in this system. Managers responsible for TSA field operations reported that they could not effectively carry out their mission with this outdated information.

- TSA systems used for incident reporting were not integrated. When an incident, such as a theft or a detected threat, occurred, TSA staff documented the incident and reported it to various offices at headquarters, such as the Transportation Security Operations Center and the Office of Security Operations. Field personnel had to enter manually the same or similar incident report information into three separate systems—the Security Incident Reporting Tool, the Airport Information

Management System, and the Performance and Results Information System.

TSA's systems do not provide the needed functionality because of challenges with the requirements gathering process. OIT Field Relations Managers are responsible for ensuring that field stakeholders' critical IT requirements are understood, prioritized, implemented, and supported. OIT Customer Relations Managers are responsible for assisting TSA operational components with documenting business requirements for IT products and services and shepherding IT project requests through TSA's IT governance process. TSA OIT senior managers, however, reported concerns about the lack of requirements gathering from the field. In addition, an internal TSA report from November 2012 stated that there did not appear to be an institutionally supported forum in which field requirements were articulated, shared, widely vetted, and synthesized into a common set of needs that would serve all airports. Field staff told us that their concerns regarding requirements were not being addressed. Some staff reported that they stopped sharing concerns, and instead developed manual workarounds.

In addition to developing manual workarounds, TSA field personnel at some sites developed systems to meet their mission needs and objectives. For example, at one airport, staff created a system called the Central Employee Database, which consolidated data from a number of TSA IT systems into a single system. This local system allowed end-users to generate real-time executive status reports, as well as daily, weekly, monthly, and annual summaries. OIT shut down this system in 2012 because of security concerns. At another airport, staff created a system to meet their management reporting and scheduling needs. The system allowed them to enter the information they needed into one central system and export it into reports seamlessly—a function not provided by the TSA scheduling system. Users told us that this system was user-friendly. The system included multiple modules for scheduling, tracking training, and other management tools, and users' access level was adjusted based on their roles.

Locally developed systems increase security and privacy risks, particularly if these systems have not been reviewed or authorized by OIT headquarters. If systems contain personally identifiable information and have not undergone the appropriate compliance, such as a privacy threshold analysis or privacy impact assessment, vulnerabilities may exist that may put this information at risk and

lead to violations of the Privacy Act.[15] Further, since a locally developed system may not be reviewed by TSA system security personnel, its use could compromise network security through malicious network intrusions. In addition, when field staff must undertake manual processes to obtain the information they need, they are less able to meet critical mission objectives in a timely and efficient manner. For example, when screeners have to spend time manually entering data into systems or manipulating data for the information they need, there are fewer personnel available to serve at security checkpoints.

IT Support

IT specialist roles are not well defined or communicated, and the number of IT support staff is not sufficient to support users at certain field sites. IT specialists are contracted support staff who provide user, hardware, and communications support at an airport or designated field site. Not all managers responsible for oversight of IT specialists and key decision-makers were fully aware of IT specialists' roles and responsibilities. According to managers in the field, under the IT Infrastructure Program contract, IT specialists reported directly to the contractor, but their day-to-day activities on-site typically were overseen by a Federal employee IT point of contact. Some Federal IT points of contact with whom we met, however, were not able to access the contract or did not know the roles or responsibilities of IT specialists. As a result, these managers could not make sure they were using the IT specialists effectively.

Some IT specialists also were not fully aware of their roles and responsibilities. One IT specialist told us that IT specialists frequently strayed from the specifics of the contract, and that the IT specialist's role was different at different TSA field locations, despite roles and responsibilities being universal and specified under a single, enterprise-wide contract. In addition, some TSA staff were unaware of the roles of IT specialists, and therefore their expectations of the IT specialists sometimes differed from officially assigned roles.

Additionally, the number of IT support staff was not sufficient to support users at certain field sites. At the time of our fieldwork, TSA employed 89 IT specialists,

[15] A privacy threshold analysis is performed to determine if additional privacy compliance documentation is required, such as a privacy impact assessment. A privacy impact assessment documents what personally identifiable information the Department is collecting, why it is being collected, and how it will be used, shared, accessed, and stored.

who were assigned to Category X and Category I airports.[16] The ratio of IT specialists to the number of users supported, however, varied significantly at different locations. For example, at Chicago Midway International Airport, one IT specialist supported approximately 200 users. At Chicago O'Hare International Airport, one IT specialist supported approximately 2,200 users. Furthermore, IT specialists may also have to travel to smaller airports. Users with whom we met sometimes had to wait several hours or more for IT support for a time-sensitive, mission-critical, or otherwise urgent task, even when an IT specialist was on site, and staff sometimes waited several days or a week for help with their requests for IT support.

To fill gaps in IT support staff, several field sites detailed employees from other operational areas. Staff detailed to help IT support in TSA field sites were frequently security officers or screeners, not IT specialists. In their IT roles, these security officers or other operational staff members provided support to users by fixing computers, setting up networks, and developing and administering local IT systems. While serving in an IT support capacity, these operational staff were no longer performing their originally assigned security or screening duties. In addition, these staff may not be qualified or trained to serve in IT support functions. By reducing the number of available personnel for security checkpoints, as well as placing staff in positions that require a specific technical training, TSA may hinder its ability to carry out its transportation security mission.

Recommendations

We recommend that the Deputy Administrator, Transportation Security Administration, direct the Chief Information Officer, Transportation Security Administration, to:

Recommendation #3:

Develop and implement a process to capture IT requirements in the field.

[16] TSA classifies the Nation's airports into one of five categories (X, I, II, III, and IV) based on various factors such as the number of takeoffs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings, and Category IV airports have the smallest.

Recommendation #4:

Communicate the IT specialist role, as contractually defined, to both IT specialists and to the user community.

Recommendation #5:

Develop and implement a process to provide sufficient IT support, such as an appropriate number of IT specialists, in airports and operational sites in the field.

Management Comments and OIG Analysis

The Administrator, Transportation Security Administration, concurred with our recommendations and provided details on steps being taken to address specific findings and recommendations in the report. We have reviewed management's comments and provided an evaluation of the issues outlined in the comments below.

In response to recommendation three, the Administrator concurred and stated that the TSA OIT and Office of Security Operations will jointly produce procedures to improve the requirements definition and development process. The Administrator also provided details about initiatives underway for identifying requirements in the field, such as the implementation of a documented process for all programmatic requests to support TSA customers in the field and the Deputy CIO's regularly scheduled bi-weekly site visits to various airports as another means for identifying requirements in the field. We recognize these actions as positive steps toward addressing this recommendation, and look forward to learning more about progress in improving the requirements definition and development process. This recommendation will remain open pending evidence of further progress in this regard.

In response to recommendation four, the Administrator concurred with the recommendation and stated that TSA has already taken action to communicate the IT specialist role, by providing a nonproprietary synopsis of IT support duties to new Federal Security Directors, as well as Federal Security Directors and senior local staff upon request. Further, the Administrator stated that a nonproprietary synopsis of those duties will be posted on the OIT/End User Services/IT Field Services Branch SharePoint site, to which all IT Specialists and

locally assigned IT points of contacts have access. We recognize these actions as positive steps toward addressing this recommendation, and look forward to learning more about progress made toward communicating the IT specialist role, as contractually defined, to both IT specialists and the user community. This recommendation will remain open pending evidence of further progress in this regard.

In response to recommendation five, the Administrator concurred with the recommendation. The Administrator said that primary IT support for Category X and I airports is provided by an on-site IT Specialist, who also provides secondary support to spokes (Category II-IV airports) of their hub airport and may assist at other sites; primary support for Category II-IV airports is provided by dispatched Field Equipment Service Support technicians. The Administrator said that the field support is dependent upon available funding for these support services, and that the current service model is the most efficient and effective employment of IT resources in support of all category airports. We recognize that field support is dependent upon available funding, and look forward to learning about progress made toward addressing this recommendation. This recommendation will remain open pending evidence of further progress in this regard.

Appendix A
Objectives, Scope, and Methodology

The DHS Office of Inspector General 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.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted an audit to determine TSA's progress in establishing key IT management capabilities to support mission needs.

We researched and reviewed Federal laws, management directives, and agency plans and strategies related to IT systems, management, and governance. We obtained published reports, documents, and news articles regarding TSA's management and use of IT. Additionally, we reviewed recent GAO and DHS OIG reports to identify prior findings and recommendations. We used this information to establish a data collection approach that consisted of focused information-gathering meetings, documentation analysis, site visits, and system demonstrations to accomplish our audit objectives.

We held meetings and teleconferences with TSA staff at headquarters and field offices. Collectively, we met with more than 120 individuals, such as headquarters officials, field office staff, and system users, to learn about TSA's IT functions, processes, and capabilities. At headquarters, we met with TSA OIT officials including the CIO, Deputy CIO, General Managers, division directors, branch chiefs, and program managers to discuss their roles and responsibilities related to TSA IT management. We also met with staff from OIT offices and divisions, including IT Strategy and Innovation, Mission Engagement, Strategy and Enterprise Management, Enterprise Architecture, IT Operations, End User Services, Applications Development, Business Management Office, and FAMS IT.

At TSA field locations, we met with Federal Security Directors, Assistant Federal Security Directors, and their staff; coordination center managers; training managers; administrative officers; property administrators; transportation security managers; transportation security officers; and other system users to understand IT development practices, user requirements, and system use in the field. We discussed the current IT environment and the extent to which it supports mission needs, local IT development

practices, and user involvement and communication with headquarters. We collected supporting documents about TSA's IT environment, IT management functions, current initiatives, and improvement initiatives.

We conducted audit fieldwork from September 2012 to January 2013 at TSA headquarters offices in Arlington, Virginia. We conducted additional audit fieldwork at TSA field locations.

We conducted this performance audit between September 2012 and March 2013 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.

The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Richard Harsche, Director of Information Management. Major OIG contributors to the audit are identified in appendix D.

Appendix B
Management Comments to the Draft Report

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

Transportation Security Administration

MAY - 6 2013

INFORMATION

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Office of Information Technology Audits
U.S. Department of Homeland Security (DHS)

FROM: John S. Pistole
Administrator

SUBJECT: *Transportation Security Administration Information Technology Management Progress and Challenges,* OIG Project No. 12-155-ITA-TSA

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to the DHS Office of the Inspector General (OIG) draft report titled, *Transportation Security Administration Information Technology Management Progress and Challenges*, OIG Project No. 12-155-ITA-TSA.

Background

DHS conducted this performance audit between September 2012 and March 2013. The objective of the audit was to follow up on a 2007 audit to determine TSA's progress in establishing key Information Technology (IT) management capabilities to support mission needs. OIG researched and reviewed Federal laws, management directives, and Agency plans and strategies related to IT systems, management, and governance. Additionally OIG interviewed more than 120 TSA Headquarters and field management staff, including Federal Security Directors and their staff. As a result of this review, OIG concluded that the TSA Deputy Administrator direct the following: (1) all TSA program offices to apply the Department's definition of all IT for all acquisitions; (2) develop and implement a process to ensure that all IT acquisitions, including passenger and baggage screening equipment, go through IT Acquisition Review and receive enterprise architecture, security, and privacy reviews; (3) develop and implement a process to capture IT requirements in the field; (4) communicate the IT specialist role to both IT specialists and to the user community; and (5) develop and implement a process to provide sufficient IT support, such as an appropriate number of IT specialists, in airports and operational sites in the field.

Discussion

While TSA concurs with the OIG's recommendations, there is one specific area within the report on which we would like to comment.

TSA accepts the recommendation that IT acquisitions, when designated as IT, will follow the DHS IT acquisition review (ITAR) guidelines and process. TSA does not agree with the OIG's recommendation that presumes the Electronic Baggage Screening Program (EBSP) and the Passenger Screening Program (PSP) are IT programs by the phrase "including passenger and baggage screening equipment." TSA is establishing a process through our draft Management Directive 1400.20, *IT Governance* in which the Chief Information Officer (CIO), the Chief Procurement Officer Executive/Component Acquisition Executive, and the Program Office jointly evaluate the program for IT designation and apply necessary IT governance.

The recommendations highlighted in OIG's report will help TSA continue improving and implementing effective oversight of Agency investments. TSA concurs with the recommendations and has already taken steps to address them. What follows are TSA's specific responses to the recommendations contained in the OIG report.

Recommendation #1: Direct all TSA program offices to apply the Department's definition of IT for all acquisitions.

TSA concurs. TSA recognizes the need to apply the Department's definition of IT and has codified that definition in TSA Management Directive 300.15, *Information Technology Acquisition Review*. TSA's position is that while IT is an integral part of almost every program we have, there should be a mechanism for determining the application of the definition in program designations. That characteristic of IT is included in TSA's definition of IT in the Management Directive. To adjudicate the application of the definition of IT in program designation, TSA has included a process in our draft Management Directive 1400.20, *IT Governance*. That approval process involves the CIO, the Chief Procurement Officer Executive/Component Acquisition Executive, and the Program Office in the IT designation process.

Recommendation #2: Develop and implement a process to ensure that all IT acquisitions, including passenger and baggage screening equipment, go through IT Acquisition Review and receive enterprise architecture, security, and privacy reviews.

TSA concurs. TSA accepts the recommendation that IT acquisitions, when determined to be designated as IT, will follow the DHS ITAR guidelines and process. The Agency takes exception to the presumption that EBSP and PSP are IT programs. As described in Recommendation #1, TSA is establishing a process through our draft Management Directive 1400.20, *IT Governance* in which the CIO, the Chief Procurement Officer Executive/Component Acquisition Executive, and the Program Office jointly evaluate the program for IT designation. TSA has a well-established ITAR process that has been defined in TSA Management Directive 300.15, *Information Technology Acquisition Review*.

Recommendation #3: Develop and implement a process to capture IT requirements in the field.

TSA concurs. TSA has Office of Information Technology (OIT) Field Regional Managers (FRM) assigned to support all airports managed by the Office of Security Operations (OSO). These FRMs have been in place since TSA was stood up. Each of the FRMs is responsible for supporting all IT-related requests within each of their respective areas of responsibility. TSA acknowledged that the process could be refined well over a year ago, so the implementation of a documented process for all programmatic requests was established to support our customers in the field. This process allows OSO leadership to review these requests to determine if they are in fact a priority for their organization and if the funding is available to support their request. In addition, in an effort to collaborate with the field, the TSA Deputy CIO established a regularly scheduled bi-weekly site visit schedule to various airports throughout the country as another means for identifying requirements in the field. The TSA OIT and OSO will jointly produce procedures to improve the requirements definition and development process.

Recommendation #4: Communicate the IT specialist role, as contractually defined, to both IT specialists and to the user community.

TSA concurs. IT support to the field sites is a contractual requirement under the current infrastructure support contract. A nonproprietary synopsis of those duties is captured in a handout that is provided to all newly assigned Federal Security Directors (FSD) as well as all FSD and senior local staff on request. In addition, the synopsis will soon be posted on the OIT/End User Services/IT Field Services Branch SharePoint site. All IT Specialists and locally assigned IT points of contacts (POC) have access to this site. Weekly calls are conducted with TSA's FRMs, the infrastructure support contractor's Customer Service Regional Managers (CSRM), on-site IT Specialists, and local IT POC. These recurring conference calls provide a forum to address both routine tasks and emerging projects and the responsibilities associated with those tasks, if clarification is needed.

Recommendation #5: Develop and implement a process to provide sufficient IT support, such as an appropriate number of IT specialists, in airports and operational sites in the field.

TSA concurs. Primary IT support for category X and I airports is provided by an on-site IT Specialist. These IT Specialists also provide secondary support to the spokes (category II –IV airports) of their hub airport. Meanwhile, they may also assist with special projects at other sites not associated with their hub location, when required. Field Equipment Service Support (FESS) technicians may also be used to provide additional support to category X and I airports when workloads and/or special projects require additional support to meet particularly demanding operational requirements within the contract service level agreements (SLA).

Primary support for Category II – IV airports is provided by dispatched FESS technicians. These FESS technicians provide timely service from key locations across the country to airports within their prescribed service areas. Contractual SLA prescribe response times and levels of service for FESS support. These service levels and response times apply equally to all airports, category X through IV. The field support is also dependent upon available funding for these support services. The current service model is the most efficient and effective employment of IT resources in support of all category airports.

Appendix C
Definition of Information Technology

Definition of Information Technology (IT)	
Federal ***Clinger-Cohen Act of 1996, as amended (Public Law No. 104-106, Division E, February 10, 1996)***	The term "information technology" (A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract.
DHS ***DHS MD 0007.1***	Any equipment or interconnected system or subsystem of equipment/software, or any national security system, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display (including geospatial technologies), switching, interchange, transmission (wired or wireless telecommunications), or reception of data, voice, video, or information by an executive agency. For purposes of this MD, equipment is used by DHS if the equipment is used by DHS directly or is used by DHS organizational partners (including other federal agencies, state and local governments and private contractors) under a contract with DHS which (a) requires the use of such equipment, or (b) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment acquired by a contractor incidental to a contract, or equipment which contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
TSA ***TSA MD No. 300.15 IT Acquisition Review***	Any equipment or interconnected system(s) or subsystem(s) of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. Equipment can be used either directly by TSA or indirectly by a contractor performing work for the Agency that requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term IT does not include any equipment that is acquired by a contractor incidental to a contract or any equipment that contains imbedded IT that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, heating, ventilation, and air conditioning equipment, such as thermostats or temperature control devices, and medical equipment for which IT is integral to operation, are not IT.

Appendix D
Major Contributors to This Report

Richard Harsche, Division Director
Elizabeth Argeris, Audit Manager
Swati Nijhawan, Auditor-in-Charge
Daniel McGrath, Auditor
Raj Patel, Auditor
Joshua Wilshere, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator, TSA
Deputy Administrator, TSA
Chief Information Officer, TSA
Liaison, TSA
Director of Local Affairs, Office of Intergovernmental Affairs
Acting Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to: DHS Office of Inspector General, Attention: Office of Investigations Hotline, 245 Murray Drive, SW, Building 410/Mail Stop 2600, Washington, DC, 20528; or you may call 1 (800) 323-8603; or fax it directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.