DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Information Technology Management Needs to Be Strengthened at the Transportation Security Administration

OIG-08-07

October 2007

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

October 26, 2007

Preface

The Department of Homeland Security (DHS) Office of Inspector General (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.

This report addresses how well the Transportation Security Administration (TSA) manages information technology (IT) to accomplish its mission of overseeing the security of the nation's transportation systems. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CAPPS II	Computer Assisted Passenger Prescreening System
CIO	Chief Information Officer
CTO	Chief Technology Officer
DHS	Department of Homeland Security
EDS	Explosive Detection System
ETD	Explosives Trace Detection
FAMS	Federal Air Marshal Service
GAO	Government Accountability Office
Hi-SOC	High-Speed Operational Connectivity
IT	Information Technology
ITD	Information Technology Division
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
OPT	Operational Process and Technology
OST	Office of Security Technology
TSA	Transportation Security Administration
TSNM	Transportation Sector Network Management
TTAC	Transportation Threat Assessment and Credentialing

Table of Contents/Abbreviations

Figures

Executive Summary

Information technology plays a critical role in supporting the Transportation Security Administration's (TSA) security mission. Since 2001, TSA began to develop an initial IT infrastructure as well as implementing an array of explosive detection and X-ray systems to meet mission needs in key areas such as aviation security.

As part of our ongoing responsibility to assess the efficiency, effectiveness, and economy of departmental programs and operations, we reviewed TSA's IT management programs and activities. The objectives of this review were to evaluate TSA's management of current technologies and infrastructure to ensure effective transportation security mission operations and information management and exchange across internal and external stakeholders.

TSA does not manage and apply IT effectively to support accomplishment of its mission objectives. Due to early pressures to meet tight congressional time frames and the public's demand for increased transportation security, TSA's technology environment evolved quickly and in a highly decentralized manner. The resulting IT infrastructure has limited system integration and data sharing and has perpetuated inefficient manual work processes. Additionally, due to a lack of authority and standard policies to govern technology implementation across TSA offices, the agency's chief information officer (CIO) faces significant challenges in conducting agency-wide IT planning and investment management to counter the fragmented environment. The declining number of staff within the central IT Division also impedes the CIO's ability to manage the IT infrastructure and support new technology requirements. Further, TSA faces disparate aviation stakeholder challenges, such as technical limitations and privacy assurance requirements, which largely remain outside of the agency's control.

Background

The *Aviation and Transportation Security Act* (Public Law 107-71, November 19, 2001) established TSA as part of the Department of Transportation in response to the events of September 11, 2001. With the passage of this act, TSA gained responsibility for ensuring compliance with passenger and checked baggage screening regulations and deployment of security officers at approximately 450 airports. This act also called for TSA to enhance specific screening operations, such as the use of explosive detection screening for checked baggage, by December 31, 2002. Within 12 months, TSA implemented a technology and telecommunications infrastructure to meet these requirements. By the end of 2002, the agency had deployed a security operations workforce and assumed 100% of all airport screening responsibilities. In March 2003, TSA was transferred to form part of the newly established Department of Homeland Security. Figure 1 displays the timeline for these events

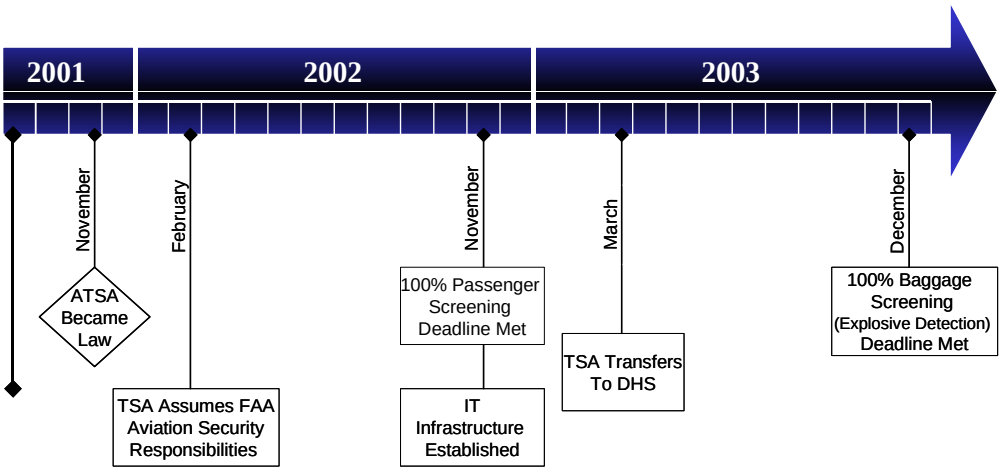

Figure 1: TSA Initial Milestones

TSA's current mission is to "protect the Nation's transportation systems to ensure freedom of movement for people and commerce," with a primary focus on the aviation sector. To accomplish this mission, the agency deploys thousands of federal air marshals, screens cargo, conducts intelligence gathering and analysis, invests in ongoing security technology research and development, manages numerous programs to improve threat identification and analysis capabilities, and disseminates information about its services to stakeholders and U.S. citizens. Leveraging new technology and partnerships with stakeholders are key factors of TSA's transportation security approach.

Today, TSA is comprised of 11 business units with nearly 50,000 employees and a budget of approximately $6.3 billion for fiscal year 2007. Foremost

among the business units, the Office of Security Operations manages the agency's primary airport field operations, as well as key security programs and frontline employees, including over 120 federal security directors and 40,000 transportation security officers. The airports that TSA serves vary considerably by size and number of passengers. The largest and busiest airports are designated as "Category X," with smaller airports falling under categories 1 through 4 (from largest to smallest). In addition, the agency has a 24-hour security operations center and 21 field offices within the Federal Air Marshal Service (FAMS) to help support airport security operations. TSA also incurred significant challenges to build supporting IT from the ground up to meet the mandated deadlines for deploying trained security officers at airports and performing screening functions.

Over the past several years, a number of audit reports have discussed key challenges relating to the management of mission critical IT programs such as Secure Flight and the Transportation Worker Identification Credential Program, along with difficulties in IT contract management:

- In February 2004, the Government Accountability Office (GAO) reported on schedule delays and poor TSA planning to develop the Computer-Assisted Passenger Prescreening System (CAPPS II), eventually leading to cancellation of the program in August 2004.[1]

- In February 2006, a GAO study of the Secure Flight program revealed that TSA had not followed a disciplined life cycle management approach in developing the new program, with potential adverse affects for its implementation.[2] As a result, the Office of Management and Budget placed the Secure Flight program on its watch list of high-risk IT programs.

- In July 2005, regarding checked baggage screening technologies, GAO reported findings that several airports were still using stand-alone baggage screening machines and explosive trace detection machines instead of more efficient in-line systems.[3] GAO determined that improved planning would be needed for optimal deployment of the more efficient screening equipment to airports.

[1] GAO, Aviation Security: *Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges,* GAO-04-385, February 2004.
[2] GAO, Aviation Security: *Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program,* GAO-06-374T, February 2006.
[3] GAO Aviation Security, *Better Planning Needed to Optimize Deployment of Checked Baggage Screening Systems,* GAO-05-896T, July 2005.

Additionally, in February 2006 we reported on TSA's management of its contract with Unisys.[4] Under this contract, Unisys was required to set up an IT infrastructure for TSA and provide IT management services. We reported that the contract had suffered significant cost overruns and delays in implementing key deliverables, such as a high-speed operational connectivity package. We also reported that the overspending and performance issues identified had resulted in part from inadequate staff to oversee and manage the contract, and we recommended rebidding the contract.

Results of Audit

Fragmented Technology Environment Lacks Integration and Standards

TSA's technology environment continues to be fragmented, hindering its ability to carry out its mission effectively. Upon creation, TSA made initial progress to establish a complete IT infrastructure, as well as a range of screening technologies for security operations at airports. However, due to time constraints, TSA's technical environment evolved in a decentralized manner, leading to stovepiped systems with limited information sharing and technical standards. Additionally, gaps in IT solutions delivery and network connectivity continue to trigger manual and inefficient processes throughout the agency.

Initial Progress Made to Establish IT Infrastructure

TSA took major steps in a short time period to establish the infrastructure and security technology solutions needed to support its newly assigned mission operations. The TSA Operational Process and Technology (OPT) office is responsible for the majority of the agency's IT and security technology functions. Specifically, as shown in Figure 2, this office administers the TSA's IT infrastructure and security technology programs, as well as business management, risk management, and strategic innovation functions.

The IT Division is responsible for managing the agency's IT infrastructure, including networks, desktops, standard applications, printers, cell phones, and peripheral hardware. To carry out these responsibilities, the IT Division oversees a range of sub-offices, including IT Security, IT Systems Innovation, IT Solutions Delivery, and the Business Management Office.

The Office of Security Technology (OST) is responsible for the agency's programs for transportation screening equipment and explosive detection

[4] DHS OIG, *Transportation Security Administration's Information Technology Managed Services Contract,* OIG-06-23, February 2006.

solutions. The primary functions of the OST are testing, deployment, and lifecycle maintenance of security technology solutions. Key sub-offices within the OST include Operations and Technical Planning, Technology Deployment and Optimization, Systems Analysis and Requirements Engineering, and Operational Integration.

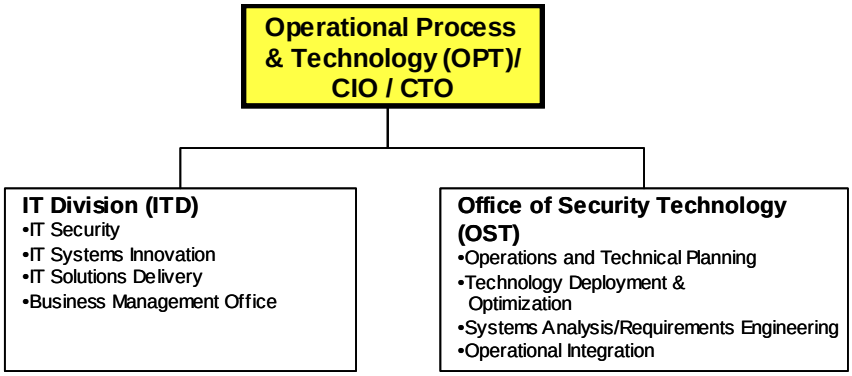

Figure 2: Operational Process and Technology Responsibilities

Beginning in 2001, the chief task of the IT Division was to establish a full-scale infrastructure within 12 months, including hardware, video, land mobile radios, phone communications, e-mail, and BlackBerry devices. By 2002, TSA had successfully implemented this IT infrastructure to support headquarters operations as well as the federal security directors and staff field locations. More recently, TSA completed a refresh of all desktops and laptops at headquarters, airports, and field offices, installing a uniform desktop image and standard lock-down policy across all sites.

TSA also has made strides in replacing dial-up communications with much needed high-speed operational connectivity (Hi-SOC) to most airports' passenger and baggage checkpoints, as well as to federal security directors' offices.[5] TSA established a plan to expand Hi-SOC to the largest airport checkpoints; as of May 2007, the agency was 70% complete in implementing this plan for passenger checkpoint areas and 57% complete for baggage screening areas. Once the high-speed connectivity is fully implemented, field locations will experience greater levels of productivity in performing daily online tasks, as well as in remotely transmitting data to TSA headquarters.

Improving contract management to help support this infrastructure has been another area of emphasis. Specifically, TSA is converting to a DHS vehicle to obtain IT support services, in efforts to overcome historical challenges with its IT managed services contract with Unisys. Specifically, the DHS Enterprise

[5] As of May 2007, TSA has established basic high-speed connectivity at 86% of the nation's category X and category 1 airports, and 99% of the nation's category 2, 3, and 4 airports.

Acquisition Gateway for Leading Edge Solutions contract is a standard, department-wide platform for acquiring IT services with improved cost efficiency and oversight. TSA will begin contracting actions in the first quarter of FY 2008 to transition to the new contract vehicle.

Meeting the aggressive congressional deadlines for implementing screening solutions was no easy undertaking. The *Aviation and Transportation Security Act* held TSA responsible for screening all passengers within 1 year from the date of enactment of the legislation, November 19, 2002, and required explosive detection screening for all checked baggage by December 31, 2002.[6] The deadline for explosive detection screening was later extended by one year.[7]

To meet this requirement, TSA's OST instituted its Passenger Screening Program and Electronic Baggage Screening Program to rapidly procure and deploy security equipment to approximately 450 airports nationwide. For electronic baggage screening, TSA's OST deployed two types of screening equipment: (1) explosive detection systems (EDS), which use X-rays to automatically recognize the characteristic signatures of threat explosives, and (2) explosives trace detection (ETD) equipment, which uses chemical analysis to detect traces of vapors and residue from explosive materials. By 2007, TSA's OST successfully deployed over 13,000 pieces of security equipment, including enhanced walk-through metal detectors, threat image X-rays, certified explosive detection systems, and explosive trace detectors.

Since these initial deployments, the TSA OST has partnered with DHS' Science and Technology Directorate for ongoing research and development to continually enhance its security technology solutions. The deployment of aviation security solutions accounts for the majority of spending within TSA's OPT office.[8] TSA also conducts ongoing pilots as part of its process for testing new security equipment. For example, TSA pilots in 2007 involved new electronic baggage systems, passenger screening equipment, and airport access control systems.

TSA has structured a Security Technology Integration Program within the OST to network its security equipment. The program will leverage Hi-SOC connectivity to establish a centralized enterprise data management system to facilitate the exchange of information between transportation security equipment located at the nation's airports and the people who use, procure, and service the equipment. The resulting unified network will support remote

[6] *Aviation and Transportation Security Act*, Public Law No. 107-71, Sec. 110, November 19, 2001.
[7] *Homeland Security Act of 2002*, Public Law No. 107-296, Sec. 425, November 25, 2002.
[8] OST spending represents $1.1 billion, of which $15.1M is categorized as IT for fiscal year 2007.

access and monitoring, reduce operations and maintenance costs, and improve efficiency by facilitating system upgrades and patch management. The program will begin in 2008 and require up to four years to complete. Figure 3 gives an example of EDS machines in a stand-alone configuration. After this program is complete, security equipment will be connected to a central network to automate data collection and provide remote monitoring capabilities.

[Source: GAO-06-869]

Figure 3: EDS Machines Used by TSA to Screen Checked Baggage

Stovepiped IT Environment Evolved

Because of the fast-paced and ad hoc manner in which TSA was established, the supporting IT infrastructure evolved in a decentralized, inefficient manner. Specifically, the infrastructure is characterized by independent IT deployments, limited systems integration, inadequate IT solutions to meet user needs, and a range of locally developed applications to fill the gaps. These technical inefficiencies have resulted in a lack of information sharing across the agency's systems, further impeding effective data management practices and workflow. TSA does not employ effective systems development and lifecycle management practices throughout the agency. Such practices would ensure that future IT systems are instituted in a more integrated and disciplined manner to support cross-agency sharing.

Independent and Non-Integrated Technology Deployments

According to Office of Management and Budget Memorandum No. 4, Circular A-130, agencies must ensure that IT planning and development activities do not duplicate existing capabilities within their organizations. However, TSA business offices have undertaken independent, parallel IT initiatives, resulting in specialized technology platforms, networks, and systems and, generally, a stovepiped IT environment across the agency. The IT Division is responsible for the basic TSA infrastructure. However, due in part to the IT Division's limited staff and budget to service TSA-wide needs, a number of component offices also have established their own IT infrastructures and support operations, as illustrated below in Figure 4.

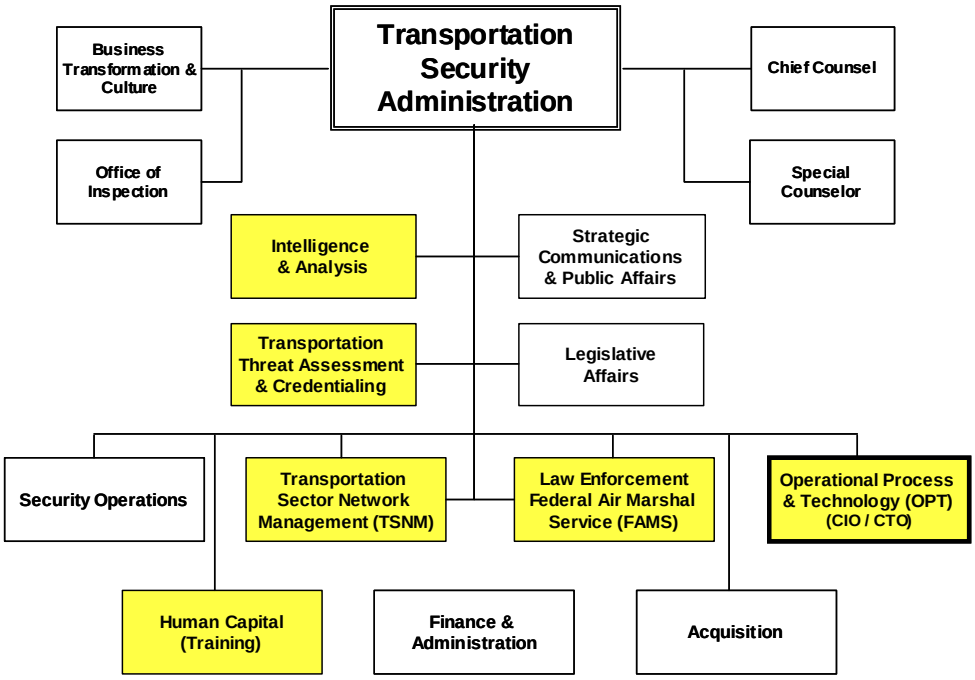

Figure 4: TSA Offices with IT Activities

For instance, the FAMS and the Office of Intelligence and Analysis are the foremost offices that have separate IT infrastructures, established in part due to their specialized mission operations and security requirements. First, the FAMS operates an independent network, and provides its own desktops, software licenses, applications, and IT support services. The FAMS began building this infrastructure after the terrorist attacks of September 11, 2001, highlighted the need for increased air transportation security. A state of the art IT infrastructure with sophisticated scheduling and communications capabilities was needed to accommodate the exponential growth in the number of FAMS agents and offices and their operations.

Second, the Office of Intelligence and Analysis also manages a separate intelligence network and telephone system. Like the FAMS, this office conducts sensitive security operations, requiring specialized communications and IT systems.

To a lesser extent, other TSA offices also have developed systems and implemented applications independently to support their specialized missions. For example, the Human Capital Office led an effort to upgrade its online training system in September 2006. Once deployed, this customized system slowed computer operations across multiple field locations and adversely affected network performance. According to IT personnel, this incident was due to inadequate system testing and configuration management. Further, IT Division management stated that ongoing problems with congestion in server and network operations are due in part to the non-integrated systems and a proliferation of spreadsheets and databases.

As a result of such IT inefficiencies, TSA has incurred increasing operations and maintenance costs. For example, the IT Division's refresh of headquarters and field office computers in 2006 did not include the FAMS offices. Rather, the FAMS' own IT organization completed a separate IT infrastructure refresh program at the same time under an independent contract. Similar instances occur throughout TSA business offices as separate contracts are established to manage major IT development efforts.

In the Transportation Threat Assessment and Credentialing (TTAC) office, where a number of contracts to develop vetting systems are managed, officials acknowledge that this approach is not cost-effective and that the systems should be supported through one consolidated contract for the organization. These parallel efforts result in an inefficient use of resources and limit the agency's opportunities to realize cost savings through enterprise-wide planning and consolidation.

Given the independent and non-integrated manner in which technology has been deployed, there is a lack of standardization among the IT platforms, hardware, and software used throughout the agency. For example, a number of offices throughout the agency have acquired phone systems, mobile devices, and peripheral hardware from different vendors. Additionally, several offices maintain separate, multiple contracts with providers of software, hardware, and application development services, as well as general services such as wireless IT.

In this fragmented technology environment, the agency has also faced challenges in obtaining enterprise-level software licenses. According to senior IT staff, if two offices require the same software or application licenses,

there is no way to bring these requirements together to serve the whole agency. Further, because most offices do not maintain a specific budget for licenses, there are project managers with $5 to $10 million projects who lack the necessary project management software. As a result, TSA remains unable to provide its staff with the necessary tools to complete their job efficiently, or realize economies of scale through consolidation of hardware or software.

In this environment, the IT Division also is limited in its ability to manage effectively a complete inventory of all of the systems developed and deployed agency-wide. Multiple inventories are maintained, each with slight variations of system names that are based on different definitions of applications, systems, and projects. Further, TSA faces difficulties in establishing a true system of record for its field equipment due to multiple databases and locally managed spreadsheets. As a result, TSA is unable to capture or maintain accurate records in systems such as its security equipment inventories, which range from 15,000 to 17,000 pieces of equipment. Such wide variations lead to an inability to document and maintain a complete picture of the existing technical environment and supporting data.

The IT Division hopes to minimize such redundant systems development activities through its new Systems Innovation Group, established to support central, CIO-led development of systems to meet common requirements across TSA. This effort supports the IT Division's goal of becoming a "preferred provider of IT services and support." However, the IT Division's efforts to rein in duplicative systems have not yet been fully extended to all TSA field locations. As of June 2007, the IT Division had deployed limited technology solutions to the field to support basic management and administrative functions.

In the absence of central IT support, field locations typically have developed their own IT systems to meet day-to-day operational needs, such as recording time and attendance, tracking lost and found items, and maintaining inventories of uniforms and seized goods. However, to the extent that such systems are networked, they could potentially pose risks to infrastructure operations. They also are an ineffective use of resources. To address these issues, the IT Division has begun documenting business requirements of the federal security directors responsible for overseeing airport security operations. The IT Division also plans to develop an updated "Federal Security Directors' Toolkit" of business applications commonly used in the field.

Limited Information Sharing and Standards

Because TSA systems often are not integrated, there is a corresponding lack of information sharing and standardization across the agency. A number of TSA applications contain duplicate information with varying degrees of completeness and accuracy. For example, although the agency's primary human resources management system contains basic employee data, the system is not interoperable with other personnel systems that need the same information. According to a senior IT official, there are more than a thousand databases at TSA, with no inventory of data across systems. Without a master record of available data, as well as standard data formats, TSA develops inconsistent information products and reports with duplicate and conflicting information. Ultimately, TSA is unable to look across all of its systems to "connect the dots" and manage information in an integrated manner.

The agency also maintains multiple data centers without a unified strategy, vision, or oversight. For example, TTAC runs two data centers at Annapolis Junction, Maryland, and Colorado Springs, Colorado, while the IT Division hosts its own data center in St. Louis, Missouri. Though TSA IT personnel stated the Colorado Springs Data Center serves specific operational and security needs, other TSA officials were not able to provide clear reasons for the various data centers. Although DHS is trying to consolidate its data centers department-wide, TSA has not issued guidance on merging data centers within the component agency.

With limited enterprise-wide IT systems and information management practices, TSA lacks a rigorous and disciplined approach to program management. IT initiatives typically are managed independently without enforceable standards or guidance. Although the IT Division has created some tools and standards, such as a system development life cycle management methodology, these are only partially utilized across TSA offices. According to TSA officials, some project managers do not understand how to use the methodology; the guidance needs to be tailored or simplified to promote its use. As GAO reported in February 2006, TSA's failure to follow a disciplined life cycle management approach hindered success of the Secure Flight program.[9]

The IT Division has placed priority on developing a TSA Information Sharing Environment to address these information management issues. This initiative is intended to increase data integration and standardization by moving to a

[9] GAO Aviation Security: *Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program*, GAO-06-374T, February 2006.

more flexible IT architecture. With this program, the IT Division plans to integrate independent databases so that information across systems can be accessed via a central location. Although a TSA Information Sharing Environment Roadmap was developed and funded in FY 2006, the allocation for this initiative has been reduced by over $16 million in the FY 2007 budget plan and next steps have been put on hold. Without leadership support for this effort, TSA remains challenged in following industry- and DHS-recommended practices for data sharing.

Inefficient Manual Processes Remain

Federal guidelines require that agencies improve the effectiveness of their mission operations. However, the gaps in systems development and connectivity discussed above have led to a number of labor-intensive and inefficient processes. The agency spends a significant amount of time on manually collecting data to measure performance, manage security equipment configurations, and carry out administrative functions. Key processes such as TSA watch list implementation also are not well automated.

Data Collection and Configuration Management for Security Equipment

Because TSA screening equipment is not networked, daily processes to collect data on security operations create several challenges for TSA field personnel. Currently, airport staff must collect and compile performance management data from all transportation screening equipment and transfer it to the CTO's website in a manner that is often unstructured and manually intensive. Since each type of equipment has its own unique method for collecting, storing, and downloading data, the manual nature of this part of the process permits gaps and inaccuracy in the raw data. Field officials must visit each explosive screening device and walk-through metal detector every hour to take a reading and log the data. This information is rolled up into daily reports for each airport, then e-mailed or faxed to headquarters for input to the national performance management system.

As a whole, this process for collecting data from the equipment is cumbersome, time consuming, and labor intensive. Officials at one field location estimated that it takes 10 minutes of every hour to gather the data from each walk-through metal detector. Officials at another airport estimated that their transportation security officers annually dedicate 2,920 staff hours to performance data gathering. Because the manual process is subject to errors, analysts spend approximately 2 hours each day reconciling the performance data before submitting it to headquarters.

TSA's existing configuration management processes for transportation security equipment are completely manual. For example, when changes (such as user names) are required in equipment configuration, TSA staff must physically visit each security component to make the updates. A field official must open each machine one at a time and enter the user name via a small keyboard. Additionally, given airports' changing security needs, field staff often move the security equipment from checkpoint to checkpoint, especially when the units are highly portable. As such, TSA field personnel must maintain an accurate record of the location of each piece of equipment and its authorized users. Supervisory staff complete the required paperwork on the changes in equipment location and send it to the appropriate offices at TSA headquarters.

TSA plans to address these inefficient processes and reduce the time and effort required to update security equipment. As previously discussed, the agency has begun deploying high-speed connectivity at all airports via its Hi-SOC program. TSA will build on this program by undertaking a Security Technology Integration Program to network the transportation security equipment, linking it to TSA headquarters. Once completed, this will enable TSA to streamline its performance measurement process by allowing the automatic collection of operational data from equipment. The programs will also support remote monitoring, diagnosis, and troubleshooting of checked baggage and passenger screening equipment. Overall, the OST believes that these programs will enhance security, improve resource management, and decrease operational costs.

Administrative Functions Need Improvement

As a result of deficiencies in TSA's current online training system, TSA field personnel use various methods, such as paper logs or spreadsheets, to track employee training hours. According to a number of personnel, the current online training system does not provide an accurate tool for tracking coursework and ensuring that employees complete the hours required for their training and development. As a result, TSA employees do not consistently receive full credit for hours taken and courses completed. To avoid such errors, training coordinators currently enter course hours manually, leading to potential mistakes and adverse effects on employees' performance ratings.

Additionally, headquarters is unable to automatically update training software in the field due to the lack of network connectivity. As a result, the training coordinator must use compact disks to install software updates to each training computer, sometimes at multiple off-site locations each month. According to field personnel, it may take an hour and a half to update each

computer, creating a significant burden given that there may be as many as 100 computers at a single location.

TSA Watch List Manual Procedures Create Security Concerns

Manual procedures for maintaining and disseminating the TSA watch list to stakeholders create security concerns and additional work for headquarters and field personnel. As shown in Figure 5, the TSA watch list process begins at the Terrorist Screening Center, which compiles information from across all federal stakeholder agencies and then provides a subset of this data to TSA. After receiving this information, TSA's Office of Intelligence and Analysis merges it with the agency's no-fly list. TSA standardizes the data, puts it in Microsoft Excel format, and then posts it to a TSA web board on a daily basis. Airlines have the option of using the spreadsheet manually or downloading it to their respective systems. While this process was intended to be a temporary solution, it has been in place since 2002 and its replacement remains uncertain. Proposed replacements (i.e., Secure Flight and its predecessor, CAPPS II) have experienced long delays due to program management challenges.

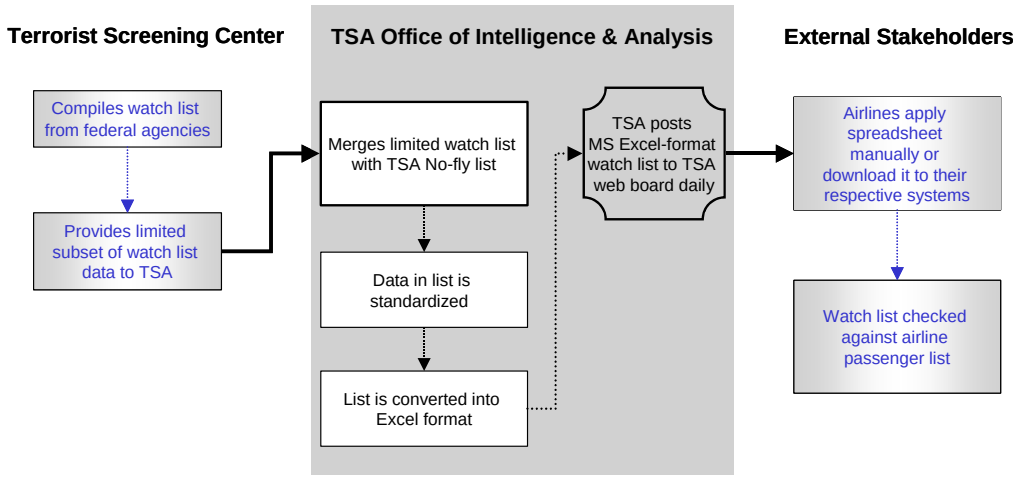

Figure 5: Process to Compile TSA Watch List

Until the current watch list process is replaced, TSA and its stakeholders face additional work to disseminate the list, as well as control access and ensure security once it is distributed. Specifically, because the list is downloaded in the form of a spreadsheet, the watch list can easily be e-mailed or printed by unauthorized parties.

Additional security concerns arise due to the fact that every airline implements the watch list differently; downloading the list is a manual process

with no clear guidance on proper use. It also is unclear how stakeholders such as airlines should implement the list. For example, there are no standard procedures or guidelines for checking an individual's name against those on the list. One airline may check multiple spellings of a name, while another airline may simply check one spelling. Additionally, at smaller airlines, employees may manually check names against a spreadsheet, which can lead to human error.

Decentralized Agency Structure Impedes Efficient IT Management

TSA has yet to institute management controls effectively to ensure sufficient levels of IT oversight and guidance to its disparate offices. Although a cohesive agency-wide IT investment review process is in the early stages of development, TSA's IT budgeting and program management functions remain scattered across a number of offices without adequate CIO oversight. Likewise, IT strategic planning remains uncoordinated, resulting in inadequate alignment of the various agencies' technology plans with agency- and department-wide strategies. Further, a number of offices maintain their own IT staff because the IT Division has inadequate resources to support the users and technology requirements of TSA's specialized business operations.

Limited Agency-Wide IT Oversight and Authority

The *Clinger-Cohen Act* (Public Law 104-106, February 10, 1996) requires that federal CIOs ensure that IT is acquired and managed in accordance with agency missions and policies. However, there is a lack of agency-wide authority and control of IT resources within TSA. Although TSA has taken steps to strengthen its IT governance and acquisition processes, technology investments are managed in a decentralized fashion across the organization.

Investment and Program Management Structure

TSA has established an acquisition process and supporting governance structure, but has not yet instituted mechanisms for consistent oversight of agency-wide IT resources and initiatives. TSA's IT investment review process is defined by DHS guidance,[10] the TSA acquisition program management process,[11] and CIO IT review guidance.[12] The agency's acquisition structure is comprised of various review boards that oversee and approve investments at key decision points throughout their lifecycles. One such board, the Business Management Council, is co-chaired by the TSA

[10] DHS Management Directive 1400, *Investment Review Process*, March 15, 2007.
[11] TSA Management Directive 300.8, *Acquisition Program Planning, Review and Reporting.*
[12] TSA CIO IT Acquisition Review Guidance V1.1, April 2007.

Chief Procurement Officer and the TSA CIO. The Investment Review Board is chaired by the TSA Deputy Administrator and includes all TSA assistant administrators and other senior officials across the agency. These boards share responsibility for reviewing and approving all TSA acquisitions.

TSA has a well-defined process for categorizing and reviewing investments. According to the TSA Acquisition Guide, investments are placed into one of four categories based on criteria such as cost, mission, risk, and resource allocations. Investments exceeding $50 million are categorized as level 1 and 2 projects and require a greater level of documentation to prepare for multiple TSA- and DHS-level reviews. These investments are subject to review by the Business Management Council, the Investment Review Board, and several DHS governance boards, chaired at executive levels up to the Deputy Secretary. Lower-level projects (levels 3 and 4) estimated at less than $50 million require only TSA Business Management Council review.

Although TSA has begun documenting and communicating guidance on its investment review process, questions remain regarding the agency's ability to enforce the guidance consistently across TSA programs. According to a TSA official, program managers are not consistently aware of the existing review boards and have limited understanding of the decision making process. Further, Office of Acquisition personnel may not always be aware of all new programs and therefore cannot always guide them by providing information on the investment review process. Program managers' lack of knowledge about the governance structure and policies also may contribute to limited compliance with acquisition management procedures. For example, managers with programs under development or still in the conceptual stage do not always understand when and how to enter the formal review process.

The TSA CIO recognizes the need to closely partner with the Office of Acquisition to ensure involvement in IT-related investment decisions. Accordingly, the IT Division began updating IT acquisition review guidance in April 2007, however these updates have not yet been implemented. The new guidance will better integrate IT review functions with the existing acquisitions process. The guidance also reflects key changes in response to DHS' directive on IT integration and management, issued in March 2007.[13]

Additionally, the DHS directive elevates the TSA CIO's role to providing formal review and reporting on all TSA IT acquisitions over $2.5 million. Given this change, acquisitions above this threshold must first go through the TSA IT review process before going to the DHS CIO and DHS Enterprise Architecture Board for approval. The updated TSA CIO guidance pursuant to

[13] DHS Management Directive 0007.1, *Information Technology Integration and Management*, March 15, 2007.

the March 2007 directive is intended to improve coordination among business functions and give the CIO more visibility and authority regarding IT acquisitions.

Specifically, per the new guidance, the TSA CIO plans to provide a monthly report to the DHS CIO on any IT purchases under $2.5 million reviewed and approved. The IT Division's Business Management Office has worked to communicate the new guidance to the business units since its development in April 2007. Business Management Office officials have noted an increase in the number of IT acquisitions they review since this directive was implemented. By reviewing and approving each IT acquisition, the TSA CIO expects to improve IT alignment with the agency's mission and target architecture.

Decentralized Budget Management

Federal laws make an agency's CIO responsible for IT capital planning and investment management functions.[14] However, TSA's decentralized IT budget hinders visibility of IT spending across the organization. As the agency evolved in a decentralized manner over the past five years, the CIO has had no official or substantive role in budgeting or planning for IT programs initiated in other offices apart from the IT Division. As a result, the CIO frequently is not consulted on significant technology decisions and investments.

There are a number of offices TSA-wide that are comparable to the IT Division in terms of IT budget control and authority. For example, the FAMS office independently manages its IT budget, as well as its own network, projects, and infrastructure. Similarly, due to its unique mission, the TTAC office maintains its own IT budget and resources. Specifically, given the office's threat assessment and credentialing function, a number of high-profile programs, such as Secure Flight, receive direct funding through appropriations or user-generated fees. Because of its mandated funding, TTAC does not have to rely on external support from the IT Division to implement its programs. However, such mandated funding also hinders enterprise-wide, long-term IT planning, and reduces opportunities to integrate and leverage existing IT initiatives.

According to DHS Management Directive 0007.1, starting in 2009, each DHS component CIO will be responsible for preparing an IT budget that includes all IT activities within the component organization. However, the IT Division

[14] *Paperwork Reduction Act of 1995*, Public Law 104-13, May 22, 1995, Sec. 3506(h); *Clinger-Cohen Act of 1996*, Public Law 104-106, Feb 10, 1996, Sec. 5122-5123.

accounts for only 26% of the total technology spending across the agency. As shown in Figure 6, TSA-wide spending in FY 07 for IT and security technology reached over $1.5 billion. While the TSA IT Division office is responsible for $408 million, the OST has purview over $1.1 billion, comprising the majority of the agency's IT-related spending. This $1.1 billion covers transportation security technology equipment, programs, operations, research and development. Of the $1.1 billion, $15.1 million is allocated specifically for IT through its Security Technology Integration Program. Additionally, in FY 07, the TTAC IT budget was $44.2 million, the FAMS IT budget was $22.4 million, and the Office of Intelligence and Analysis IT budget was $3.7 million—all apart from IT Division authority and control.

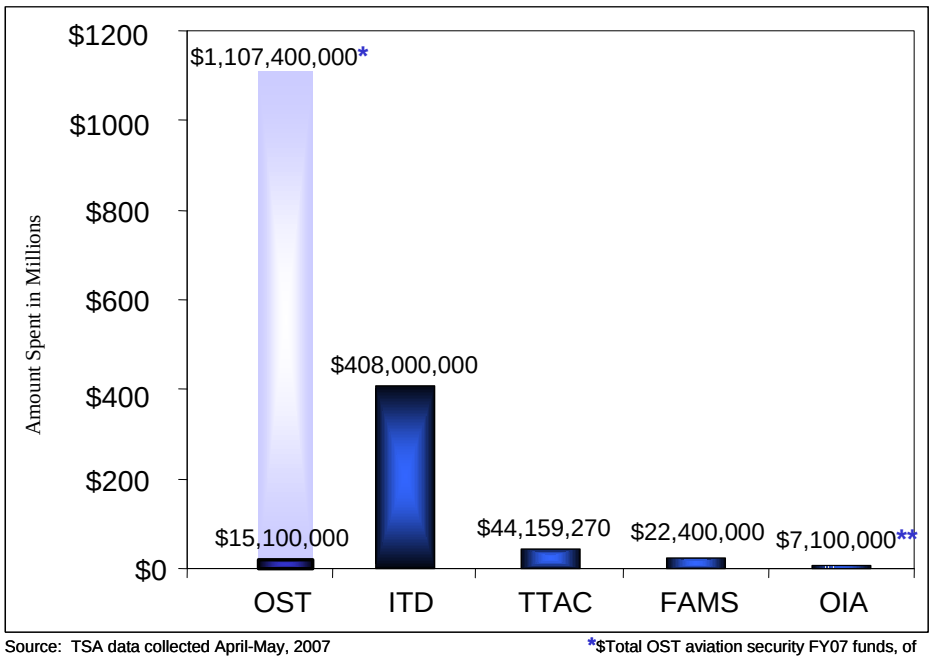

Figure 6: FY 07 IT and Security Technology Spending Across TSA Offices

Since the agency's inception, TSA offices have struggled to reach consensus on a shared definition of IT to help in consistently classifying and tracking IT spending across TSA component offices. TSA historically has relied on a vague definition of IT, based on Office of Management and Budget Circular A-11 and the *Clinger-Cohen Act*. Currently, airport security technology equipment, such as EDS and ETD machines, is not considered IT. In this structure, the OST manages security technology equipment and programs separate from the IT Division's traditional IT infrastructure systems. However, a number of TSA officials expressed confusion and offered conflicting opinions on what constitutes IT in the absence of clear TSA definitions and guidance. In March 2007, however, DHS provided an updated

definition of IT in its DHS Management Directive 0007.1. According to TSA officials, this directive may help to address the previous ambiguity, but its impact remains to be seen.

Delineation of what constitutes IT also is a major issue as it relates to the acquisition process. With the IT Division's help, the Office of Acquisition screens new programs to determine whether they are IT initiatives. Investments deemed "non-IT" are not subject to the same level of documentation or technical reviews as IT programs. Further, the CIO has limited involvement in "non-IT" programs, which hinders the possibility of leveraging or integrating existing solutions.

Coordination with Business Offices Is Limited

Several TSA officials said that there is a general need for more effective coordination between the IT Division and business offices. Because many TSA IT programs are not managed or funded within the CIO's purview, the CIO's ability to monitor program progress or coordinate with business units is sporadic and often "too little, too late." According to several IT officials, when business units develop systems independently of the IT Division, this presents challenges for the CIO. Deploying new systems on the network without prior coordination creates anxiety as to whether the systems will operate in the existing environment, meet security standards, or incur additional cost to incorporate redundant IT elements.

According to multiple TSA senior executives, there is no official, including the CIO, with a central purview over all IT across the agency. Rather, coordination between the IT Division and business managers often is done on an ad hoc basis or through established working relationships. Some IT Division staff said that their awareness of major IT projects often is derived from the IT security process with projects only becoming visible as they undergo certification and accreditation. One IT staff member said that the IT Division gets more information on TSA's major IT projects, such as Secure Flight, from the news media than from within the agency. In fact, IT management recently designated a contractor to monitor the internet to maintain awareness of new IT initiatives across TSA.

Immature IT Strategies, Policies, and Guidance

As with investment management, TSA has not instituted a focused approach to formulating overarching IT strategic goals, policies, or guidance to achieve mission outcomes. IT strategic planning is conducted in a decentralized manner across the organization without cohesive direction or supporting policies to ensure alignment. Although the agency has recently begun

instituting IT management tools such as an enterprise architecture to increase integration and standards for the IT environment, the tools are not yet fully developed or implemented. Further, IT support services are decentralized across a number of different offices, because the IT Division's limited resources have prevented it from serving as a central source of IT support.

TSA Needs Effective IT Planning and Management

The *Government Performance and Results Act of 1993* (Public Law 103-62, August 3, 1993) holds federal agencies responsible for strategic planning to ensure efficient and effective operations and use of resources to achieve mission results. Further, the *Clinger-Cohen Act* requires agencies to develop and maintain an integrated, enterprise-wide architecture for the agency. Developing this enterprise architecture would define and set the standards for executing the agency strategy and implementing the systems and technologies in an integrated manner to accomplish mission goals.

However, TSA has not institutionalized an effective IT strategic planning process to support an agency-wide vision or agency-wide goals and objectives. Rather, competing plans have been developed in different parts of the organization. Specifically, both the IT Division and the OST, its counterpart, have developed strategic plans. Both plans have been implemented and are in use to guide IT within the respective offices. However, there is no clear correlation between the two plans. For example, the FY 2005 to 2006 CTO strategic plan is focused on achieving TSA's mission by providing security technology solutions.[15] In contrast, the IT Division's FY 2006 to 2008 strategic plan outlines an internally focused vision that includes collaboration among TSA's business units and the IT Division becoming TSA's preferred IT services provider.[16]

Within the overarching OPT office that brings the IT Division and CTO operations together, planning officials hope to update and develop a single strategic plan for all TSA offices that strengthens IT alignment with the agency-wide strategy. However, this OPT planning effort is ongoing, with a target completion date of December 2007.

Similarly, business planning also is performed at the office level across the agency. These plans are at various stages of completion or execution. For example, the FAMS and Transportation Sector Network Management (TSNM) develop and maintain their own strategic plans due to the size and

[15] *TSA Chief Technology Officer Strategic Plan*, FY 2005–2006.
[16] *TSA Information Technology Division Strategy*, FY 2006–2008.

organizational structure of these offices. Specifically, TSNM has 10 transportation modes within the office that must consolidate planning efforts.

Because of the decentralized IT planning, there is no long-term, unified vision for aligning IT investments and programs within the agency. According to one official, the agency has only a near-term, tactical view by which to operate. For instance, although TSA has begun planning the "checkpoint of the future," which is a set of long-term goals for security checkpoints, TSA has not refined this vision to outline how security screening operations will be supported by technology. There has been much speculation among field directors regarding whether this vision will involve cutting edge technologies or redesigned processes and operations. Without a clear vision, it will be difficult to get participation and buy-in from across the agency for an enhanced security screening approach.

Lacking a unified IT strategy, there also is no way to align TSA's disparate IT initiatives and resources with the strategies of the overarching department and agency. IT alignment is important to better enable each TSA office and business unit to carry out its role in support of DHS' homeland security mission. Further, IT alignment with the TSA vision will help ensure that each office and business unit is progressing toward accomplishing the agency's goals and objectives. However, senior IT officials stated that the methods for achieving such strategic alignment are limited while the organization is still evolving. In the past year, TSA has established a Strategic Planning Office within the Finance and Administration office, which is taking a "grassroots" approach to leveraging the lower-level office and business unit plans to build one high-level strategic plan.

Additionally, TSA has not yet instituted an enterprise architecture as a framework for transitioning from its stovepiped and redundant systems to an integrated IT environment. Since FY 2005, TSA has made strides in developing its enterprise architecture to help analyze business and IT needs; however, the framework has not yet been fully developed or employed.

The IT Division's Business Management Office, responsible for the enterprise architecture effort, is in the initial stages of defining the existing "as-is" environment. As part of this effort, senior TSA officials are focused on mapping the business processes of federal security directors in the field and outlining credentialing operations within TTAC. Subsequently, the agency will define the future "to-be" state and develop a transition plan. TSA's recent award of a new contract for enterprise architecture support and development has demonstrated increased focus on this effort. Once it is completed, the IT Division plans to use the architecture within the IT review

process as a tool for aligning services to needs and identifying technical risks.

IT Support Services Are Decentralized

Although the IT Division's vision is to be TSA's "preferred IT provider," business offices throughout TSA currently provide their own IT support in a variety of ways. These independent support services have evolved in part because the IT Division has not had the staff or issued the guidance needed to support TSA-wide IT operations effectively.

Since its inception, the IT Division has faced the daunting challenge of delivering IT support despite a chronic lack of staff. In general, staffing trends in the IT Division have remained level over the years. Specifically, the IT Division has about 132 full-time government staff managing IT for approximately 50,000 total TSA employees. However, these staffing levels have not been adequate for the IT Division to meet the mission and administrative needs of other TSA offices, such as IT procurement guidance, tailored technology solutions, and dedicated technical staff support. For example, TSA's Office of Redress approached the IT Division for help in developing a system that would allow airline passengers to submit online requests for their names to be cleared from TSA's No Fly List, but the IT Division could not provide timely assistance due to its resource limitations. As a result, the Office of Redress hired its own contractor, who built a system that contained significant security flaws when launched.

Additionally, because basic infrastructure support has been the IT Division's priority to date, the IT Division has not been able to focus on developing and supporting customized applications to benefit specialized business needs. For example, soon after TSA began operations, the Human Capital Office wanted to acquire a system to track human resources data. Because the IT Division was not able to divert staff to support this project, Human Capital procured its own system and hired its own technical support personnel to manage it.

To complicate matters, despite the staffing shortfalls, IT Division workloads have increased over time commensurate with agency growth. The IT Division has relied on contractor support and managed services to provide the level of IT service and support necessary for an agency of TSA's size and scope. At the same time, the number of full-time government employees in the IT Division has been slipping over time due to attrition. Program officials said that staffing levels really should be increasing to meet the increased workloads and targeted service goals and to allow adequate oversight of contractors. In the opinion of senior IT management, the number of employees needed to accomplish IT Division responsibilities is 250 to 300—nearly double the current government workforce. As illustrated at Figure 7,

the IT Division's budget has steadily increased, which could accommodate an increase in IT support staff and services.

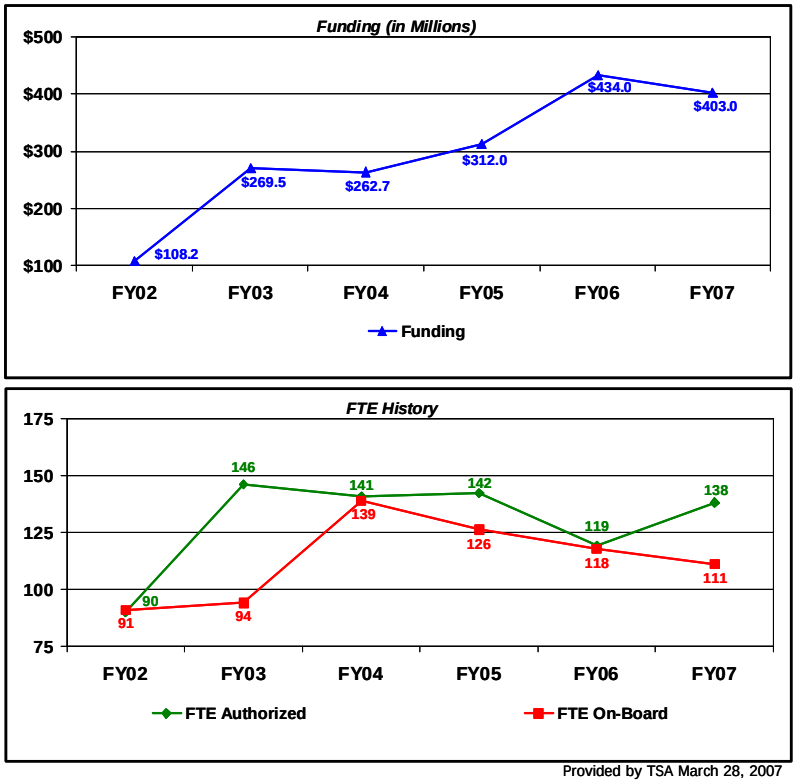

Figure 7: IT Division Funding to FTE History

However, the IT Division has not received the FTE authorizations needed, commensurate with the budget increases. According to senior technology officials, TSA leadership must first give permission for program dollars to be used for hiring full-time employees. However, there is a lack of confidence within the agency that the IT Division is capable of going beyond its historical role of basic infrastructure support to deliver a fuller range of services. Officials attributed this lack of confidence, in part, to the poor performance of the IT managed services contract.

Lacking adequate support from the IT Division, a number of TSA offices employ their own specialized IT support units. These offices justify the need for their own support services by citing factors such as unique mission or business operations or IT Division limitations. For example, the FAMS office has established an IT staff of 13 to manage its infrastructure and network and oversee contractors. Similarly, the TTAC office has an IT staff of 10 to provide technical expertise for contract oversight and support the office's operations. In addition, the TSNM office has its own staff of IT specialists

who provide support for the 10 different modes of transportation under TSNM, as well as priority support services for executive management. Although these separate IT support staffs are considered necessary to support the agency's mission, they also lead to duplicative efforts and expenses, inefficiencies, and a lack of standard processes and practices.

IT Division management hopes to rein in these disparate IT support resources by widening the range of services that they offer and increasing the reliance of the business units on the IT Division over the coming year. For example, the IT Division plans to expand its services to include more development and customization of applications to meet business unit needs. As part of this effort, the IT Division also will leverage the newly increased network connectivity to improve the effectiveness of new and continuing IT initiatives.

To further its relationships with the business units, the IT Division has assigned an account manager to work with each TSA business office and serve as a liaison for meeting IT needs. IT Division management anticipates that the benefits of this arrangement will include increased awareness of the customer's business and technical needs, particularly in terms of developing and gathering requirements. Additionally, this approach is intended to build the reputation of the IT Division, and to increase its visibility throughout the organization.

As of October 2006, the IT Division had begun implementing plans and applied $3 million in FY 2007 funds to support the account manager approach. Initial reception of this approach has been positive, and business units are communicating through the account managers to bring more issues to light. The IT Division continues to define the account manager's role to further enhance inter-office working relationships and ensure effective IT service delivery.

Numerous Challenges Exist in External Stakeholder Coordination

Coordinating with transportation systems stakeholders is a major challenge for TSA. A number of federal laws, including the *Homeland Security Act of 2002* (Public Law 107-296, Nov. 25, 2002) and the *Aviation and Transportation Security Act*, govern how the agency must partner with stakeholders to carry out its transportation security operations. Taken together, these laws require that the agency carefully mete out its limited financial and administrative resources to address the needs of each stakeholder on an individual basis. TSA's challenges in meeting these responsibilities, as illustrated in Figure 8, include:

- Balancing the competing interests of numerous external organizations whose missions and operations are inherently different from one another strains TSA resources and budgets.
- Applying customized solutions to accommodate varying requirements due to differences in stakeholder facilities, capabilities, and technology.
- Communicating with stakeholders effectively on the guidelines for obtaining funding and meeting transportation security technology standards.
- Meeting federal requirements and public concerns about data privacy and security to satisfy stakeholder needs.

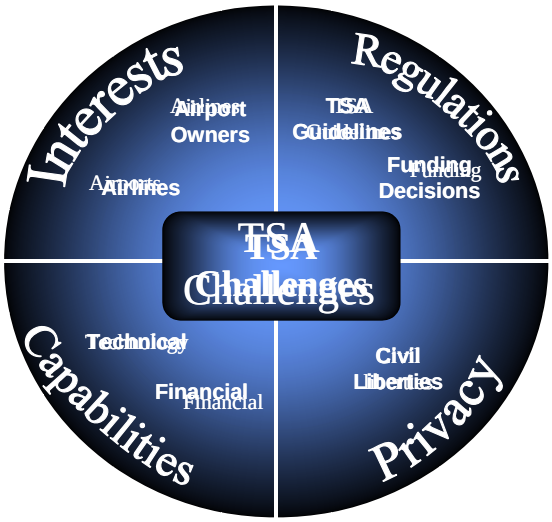

Figure 8: TSA's Challenges in Stakeholder Coordination

Addressing these challenges may improve TSA's ability to move from a reactive to a proactive approach in applying resources to meet priority requirements. Although a number of the challenges may be beyond TSA's control in some respects, the agency nonetheless can increase its ability to respond to unique stakeholder requirements by ensuring that clear transportation security technology guidelines and funding criteria are communicated and consistently applied. Additionally, identifying and devising strategies in advance to mitigate the risks of compromise or unauthorized disclosure of personally identifiable information can also alleviate concerns about the privacy and security of TSA data.

Meeting Stakeholders' Diverging Interests

Collaborating and interacting with multiple stakeholders to design and deploy screening technologies to over 450 airport facilities is no easy task for TSA. The challenge arises from the fact that the stakeholders, including airport

owners and operators as well as commercial airlines and their customers, have differing interests, responsibilities, and priorities.

For example, TSA must consider a number of factors in designing and implementing screening solutions to meet airports' interests and operational needs. Most airports are owned by state or local governments and operated by government-funded airport authorities and must focus on meeting community and taxpayer needs. As such, they are concerned with controlling costs, managing revenue flows, and serving the traveling customer. At the same time, however, airports must place a premium on ensuring safety and preventing transportation security incidents.

TSA often is caught in a dilemma in working to ensure aviation security concurrent with meeting the airports' divergent operational and customer service needs. For example, the complex screening equipment that TSA deploys to help ensure aviation security often is extremely heavy and bulky, and consumes a considerable amount of space. Airports with space or building engineering constraints sometimes must place the equipment in lobby areas, increasing congestion and passenger processing times. This incursion also poses public safety issues, since crowded spaces are difficult to monitor and patrol.

In addition, airports may lose income when security checkpoint or baggage screening equipment takes up valuable retail space that could be used for more profitable operations, such as food courts or parking lots. Further, one TSA official said that while deploying backup screening equipment on site meets the airports' concern about guarding against service disruptions, TSA finds it difficult to justify the redundant expense for the equipment because it is rarely used.

Conversely, TSA is challenged in its efforts to balance aviation security with the profit motive of commercial airlines. While airlines, too, are concerned with security, as private companies they are primarily focused on business and performance goals, reputation, and customer service, which affect revenue. For example, one airline representative said that frequent TSA baggage screening equipment failures during morning rush hour peak times result in flight delays and tens of thousands of dollars in additional operating costs. An airline official told us about another instance where TSA equipment breakdowns led to about 50 bags not making it onto a flight, inconveniencing passengers and causing increased operating expenses for the airline to track and ship the delayed luggage.

In addition, several airlines provide TSA with booking information in advance to assist in scheduling the appropriate number of screening personnel for duty

and help alleviate long passenger screening lines. However, TSA staff shortages and inability to readily adjust the shifts of federal screeners to meet workload demands may result in backed up lines at peak periods or substantial overtime costs. Such inconveniences result in customer complaints and negative perceptions of both the airlines and TSA.

Accommodating Varying Stakeholder Capabilities

Another challenge that TSA faces is designing security solutions and systems to accommodate disparities in stakeholder capabilities. Factors such as facility size, capacity, budget, current technology, and staffing affect TSA's ability to execute security operations effectively. For example, some airports have the capacity to integrate sophisticated "in-line" EDS systems with luggage conveyance systems to automate baggage screening; others are constrained by building engineering, geographic location, or airport construction or modernization plans that limit the type and amount of equipment that they can deploy. Such constraints may lead to temporary solutions or sub-optimal baggage screening arrangements where machines are placed in lobbies, temporary structures, or other less convenient areas. Further, financial resource limitations also may affect screening system designs. For example, while some airports can afford state-of-the-art screening systems, others struggle to meet minimum standards and maintain outdated equipment.

Variations in airlines' technical capabilities also hinder TSA mission execution. Technology used in critical initiatives, such as the No Fly List, which aids airlines in prescreening passengers for potential security risks, must accommodate the airlines' technical limitations. Specifically, since there is no common system across the airlines for downloading and using No Fly List data, TSA must use "lowest common denominator" technology to distribute the information. To accommodate small airlines that must view the data manually, TSA uses the simplest formats, i.e. Microsoft Excel, to disseminate the lists, although other airlines would prefer more sophisticated formats. The lack of consistent systems across airlines also means that small adjustments in data presentation, such as changes in spreadsheet column widths or capitalization of letters, can cause system crashes and considerable additional expense.

Communicating Security Regulations and Guidelines

TSA faces challenges in clearly and effectively communicating to stakeholders regarding guidelines for implementing security technology and obtaining funding. TSA is responsible for providing aviation security

guidance, such as the requirement to screen all passengers and checked baggage for air travel. Typically, TSA's approach has been to coordinate with each airport on a case-by-case basis to work through complex cost-sharing models and project scopes. TSA employs various tools such as prioritized site lists, letters of intent, and letters of prejudice, which preserve eligibility for self-funding airports to receive federal reimbursements in the future, to manage the airports' competing needs for funding and resources. However, addressing the complexities and varying conditions at the individual airports takes time and fosters reactive and uneven response to airport needs. As such, airport and airline officials have complained about a lack of clarity and consistency in policy documentation and execution.

Airports are particularly concerned about a lack of clear guidance from TSA about the implementation of in-line baggage screening systems. The airports and TSA have met previous deadlines for 100% passenger and baggage screening in accordance with the *Aviation and Transportation Security Act*.

While the 100% requirement is clear and remains in effect, the added requirement to increase automation and efficiency by replacing ETD devices and stand-alone EDS machines with in-line systems where possible is less clear. Such systems are costly, yet airport officials have said they see a lack of TSA policies on funding or implementation of these in-line baggage screening systems at airports. A TSA official confirmed that TSA has not issued such policies, but the agency has developed a framework for different levels of automation, as well as suggested solutions for 250 airports, based on their size and other characteristics. The framework also presents a prioritized list of the top 25 airports for which TSA funding assistance is planned, based on a quantitative analysis using weighted criteria.

However, a number of airport officials and TSA field personnel do not have sufficient awareness or understanding of these and other equipment and funding guidelines to make the guidelines useful. With regard to implementing and deploying security technology, airport officials said that there do not appear to be definitive or consistent processes coming from headquarters. These officials also said that the funding process is "opaque," characterized by a lack of criteria and uniform procedures for securing TSA financial assistance. Officials and TSA field personnel also were unaware of their airport's funding prioritization status. Even at airports that had received or expected to receive funding, there were ongoing negotiations and disagreements regarding what TSA would or would not fund.

Without systematic and objective guidance and procedures, airport officials often must engage in time-consuming negotiations with TSA headquarters

regarding funding and technology standards, not knowing whether their concerns will be equitably addressed. Airports encounter difficulties in long-term planning and financing of security technology improvements because officials do not know whether or how much TSA may eventually contribute to assist their efforts. Further, security technology improvements that airports undertake must be scaled back in some cases due to these financing uncertainties and airports' limited budgets. As a result, new screening systems and other security equipment that may be in place for years fall short of meeting TSA's performance and efficiency expectations. Since less efficient equipment requires more people to support operations, the installation of less efficient long-term systems also results in continued high staffing needs and expenses for TSA.

Addressing Data Privacy Concerns

Establishing the appropriate balance between executing mission responsibilities and respecting the privacy and legal rights of the public is a challenge for TSA as it develops new security systems and implements pilot programs. For example, in 2002, TSA identified a new screening technology called "backscatter" as a solution to improve detection of concealed threat items such as liquids and plastics. However, the system's X-ray capability has raised privacy concerns regarding protection of the images generated by the equipment. As a result, the agency delayed the launch of a pilot program and eventually applied privacy filters to reduce body image output.

The Secure Flight program also has faced numerous challenges in responding to concerns about its ability to safeguard personally identifiable information. The program is intended to replace the No Fly List by creating a consistent platform for consolidating watch list data and prescreening passengers. However, concerns have been raised regarding the ability of U.S. passengers to seek redress from TSA if they are selected for additional screening or denied boarding privileges due to incorrect name matches identified by Secure Flight or the interim No Fly List procedures. These concerns were heightened in February 2007 when TSA launched a website through which passengers could submit online redress requests. The initial website lacked proper encryption for data submitted, as well as other information assurance features, raising questions regarding the security and validity of the site.

A recent loss of TSA computer equipment has led to further public scrutiny of the agency's ability to appropriately safeguard data that includes personal information. Specifically, on May 4, 2007, a TSA hard drive was discovered missing. The hard drive contained personal, payroll, and financial information on an estimated 100,000 current and former TSA employees.

Subsequently, some of the affected employees filed a lawsuit against the agency, charging negligence on TSA's part. Although TSA has no evidence thus far that the data has been misused, the agency determined that all affected employees would be provided with free credit monitoring for up to one year in order to prevent fraud and identity theft.

Recommendations

We recommend that the Assistant Administrator for TSA strengthen agency IT management by:

1. Empowering the CIO with agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of TSA mission objectives.

2. Developing a consolidated strategic planning approach to ensure that IT plans across the agency are well-aligned and linked to the DHS strategic plan, providing a clear vision of how information and technology will be managed to support TSA and DHS mission objectives.

3. Completing and implementing an enterprise architecture to establish technical standards and guidelines for systems acquisitions and investment decisions.

4. Establishing and communicating guidelines and procedures for acquiring, developing, and managing IT solutions in a consistent, integrated, and efficient manner.

5. Applying adequate staff resources to strengthen the IT Division in addressing IT needs and providing support to TSA operations agency-wide.

Management Comments and OIG Evaluation

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

The Assistant Secretary concurred with our recommendations and provided comments on specific areas within the report. In these comments, the Assistant Secretary explained the agency's position on whether security technology should be considered as an IT asset. Additionally, the Assistant Secretary gave examples of recent efforts to ensure coordination with stakeholders and clarified its data privacy challenges.

We have reviewed the Assistant Secretary's comments and made changes to the report as appropriate. The following is an evaluation of the issues raised, as outlined in the comments discussion provided by TSA.

TSA IT Assets

In the comments, the TSA Assistant Secretary stated concern over the inclusion of security technology equipment as part of this review of TSA's IT infrastructure. TSA stated that per the DHS Management Directive 0007.1 definition of IT, security technology equipment should not be included as IT. We are aware of this definition of IT, which was released subsequent to our initial fieldwork, and we acknowledge that the principal function of security technology equipment is for the purpose of screening persons or items. We have modified our report to ensure that security technology equipment is not specifically referred to as IT.

In reviewing TSA's IT management capabilities, we examined TSA's broad IT infrastructure, including security technology equipment, which plays a critical role in executing TSA's mission operations. We determined that as screening processes become more automated, it will be difficult for TSA to separate its security technology equipment from the agency's IT assets. For example, to better automate threat detection and handling functions, an increasing number of TSA's security-screening operations are enabled by computers using IT features such as the following:

- graphical interfaces,
- sophisticated algorithms,
- networking capabilities,
- complex software, and
- multi-dimensional image displays.

As IT and screening technologies converge, TSA will need to address, and plan for the possible impact that screening systems have on its IT infrastructure.

Additionally, regarding the budget allocation references for TSA's IT assets, TSA stated that the inclusion of the OST Passenger Screening Program and Electronic Baggage Screening Program funding activity as IT spending was misleading. TSA also said they have captured IT elements of both the Passenger Screening Program and the Electronic Baggage Screening Program into the Security Technology Integration Program budget, which is significantly less compared to the total budgets for these two screening programs. Further, TSA stated that the Office of Management and Budget has concurred with this designation of IT for the Security Technology Integration Program as recently as March 2007. We recognize that TSA has captured the IT elements of each screening program and are managing these IT functions through the Security Technology Integration Program budget. Accordingly, we have modified the report section on budget management and the related IT spending chart to reflect the IT portion of the OST total FY 07 budget.

Stakeholder Challenges

In response to stakeholder challenges pertaining to collaboration and guidance, the TSA Assistant Secretary stated that stakeholders are actively engaged on matters of airport checked baggage screening systems. Specifically, TSA stated that it has worked with industry stakeholders to develop in draft Planning Guidelines and Design Standards for Checked Baggage Inspection Systems that will be released at the end of calendar year 2007. Additionally, in June 2007, TSA issued a guide to airports applying for FY 2009 EDS system funding. We recognize recent TSA efforts to work with stakeholders to carry out its transportation security operations. However, TSA must continue to develop and communicate clear guidelines to ensure consistent level of awareness among stakeholders.

Additionally, TSA indicated that safety and privacy data protections of the new imaging technology did not lead to a delay in the field operational test and evaluation. TSA said that the delays were due to concerns with the reaction of the public regarding privacy not the actual data protection or data privacy. We modified the report to clarify the privacy concerns with the "backscatter" technology. However, data privacy remains a challenge that TSA will continue to face as they increase security operations.

Report Recommendations

The Assistant Secretary concurred with our recommendations in their entirety and stated that the recommendations will help TSA improve and implement more effective oversight of IT investments. TSA outlined a number of steps already taken to address several of the report recommendations. We believe that such efforts demonstrate progress toward addressing the various issues we raised in our report. We look forward to learning more about continued progress and improvements in the future.

In response to recommendation 1, the Assistant Secretary acknowledged the need for CIO investment review authority over TSA's IT initiatives. The Assistant Secretary stated that TSA is ensuring compliance with DHS Management Directive 0007.1 for CIO accountability of the performance, budgeting, expenditure, and staffing of the agency's IT resources. Specifically, TSA has focused on ensuring IT resources and purchasing services are included in TSA's IT portfolio and support the agency's strategic plan, business requirements, and risk management process.

Responding to recommendation 2, the Assistant Secretary said that TSA is currently updating the TSA IT Strategic Plan and it is scheduled for completion by October 2007. The new TSA IT Strategic Plan will be compliant with the TSA Strategic Plan and outline TSA's IT vision, mission, strategy, and goals through 2010.

To address recommendation 3, the Assistant Secretary stated that TSA recently awarded a contract to provide support for assessing and improving enterprise architecture management. TSA will map processes, data, applications, and infrastructure to the Federal Enterprise Architecture and TSA Strategic Goals. Eventually, this effort will consolidate common practices and data, enable consistent use of technology, reduce stovepipe solutions and redundancies, and help TSA plan for future needs.

In response to recommendation 4, the Assistant Secretary said that the TSA OCIO is transforming its business processes in accordance with DHS Management Directive 0007.1 to ensure effective management and administration of all agency IT resources and assets. Specifically, the TSA investment review process will assess all programs in terms of program alignment, enterprise architecture, IT security, and infrastructure and applications optimization.

Finally, to address recommendation 5, the Assistant Secretary stated that the TSA Office of Human Capital completed a position management review of the IT Division in August 2006 to determine appropriate staffing levels. This

review determined that the TSA IT Division required 164 full-time employees, over 30 more employees than the current staff level.

As background for this audit, we researched and reviewed federal guidance and laws related to TSA's responsibility to design, deploy, and maintain technologies to protect the nation's transportation systems. We reviewed recent GAO and OIG reports related to TSA IT systems, contracts, security, and program management. We searched the internet to obtain testimony, published reports, documents, and news articles regarding TSA operations. Using this information, we designed a data collection approach that consisted of focused interviews and documentation analysis to accomplish our audit objectives. We then developed a series of questions and discussion topics to facilitate our interviews.

Collectively, we interviewed over 90 TSA HQ and field management officials and staff to understand TSA's strategy and processes for managing IT. Officials within the IT Division told us about the current IT management environment and how it is evolving. We interviewed TSA leadership to understand the division of roles and responsibilities related to developing and implementing TSA systems. In particular, we met with OST officials to discuss the development and deployment process for aviation security technology. Additionally, we met with senior TSA officials to discuss how IT investments are budgeted and monitored across the organization. Finally, we met with program managers within several TSA offices to learn about coordination, project management, and standards in implementing major programs and IT systems.

Further, we visited five airports where we toured facilities and interviewed TSA employees such as Federal Security Directors, Training Coordinators, Security Managers, and IT Specialists to learn about their functions and operations. We discussed the current IT infrastructure, local IT development practices, and user involvement and communication with headquarters. We gathered input on the system lifecycle development and deployments, as well as performance metrics and maintenance activities.

Additionally, we met with TSA stakeholders, including airport owners and airline operators. We discussed their coordination with TSA and the extent to which they are affected by TSA decisions such as project funding, system implementations, and watch list monitoring. Finally, we met with the Transportation Security Lab in Atlantic City, New Jersey, where we discussed the ongoing development and testing of new security technologies before they are transferred for use at TSA field locations. We gathered and analyzed numerous documents that the range of TSA officials provided on IT management topics, such as systems and tools, processes and procedures, investment planning, governance oversight, infrastructure management, program planning, and budget execution.

We conducted our review from February 2007 to May 2007 at TSA headquarters in Washington, DC, and at TSA field locations in New York City (NY), Atlantic City (NJ), San Jose (CA), San Francisco (CA), and Phoenix (AZ). We performed our work according to generally accepted government auditing standards.

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 C.

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

Transportation
Security
Administration

SEP 2 0 2007

INFORMATION

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security

FROM: Kip Hawley
Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response to Department of Homeland Security (DHS) Office of Inspector General's (OIG) Draft Report Titled "Information Technology Management Needs to Be Strengthened at the Transportation Security Administration," July 2007

Purpose

This memorandum constitutes TSA's formal Agency response to the DHS OIG draft report "Information Technology Management Needs to Be Strengthened at the Transportation Security Administration," July 2007. TSA appreciates the opportunity to review and provide comments to your draft report.

Background

In December 2006, OIG began a review of TSA's information and technology management to support its mission of securing the Nation's transportation systems. The objectives of this audit were to: (1) assess TSA's information technology (IT) systems, management, and operations; (2) examine the Agency's IT organization structure, strategies, and policies for accomplishing its transportation security mission; and (3) identify the Agency's challenges in coordinating transportation security systems and information with internal and external stakeholders.

OIG interviewed more than 90 TSA headquarters and field management officials and staff and TSA stakeholders, including airport owners and airline operators, and conducted site visits at five airports. As a result of this review, OIG concluded that TSA's IT infrastructure has limited system integration and data sharing; IT planning is challenging due to the fragmented environment of the Agency; declining staff impedes the Agency's ability to manage infrastructure and support new requirements; and the Agency faces stakeholder challenges, such as technical limitation and privacy assurance requirements.

Discussion

While TSA generally concurs with OIG's recommendations, there are a few specific areas within the report on which we would like to provide comment. IT plays a critical role in supporting TSA's security mission. Since 2001, TSA began to develop an initial IT infrastructure and deployed an array of explosives detection and x-ray systems to meet mission needs in key areas such as aviation security. There are multiple areas in the report where Security Technology equipment (Explosives Detection System (EDS) machines, Explosives Trace Detection machines, etc.) is referred to as IT. DHS Management Directive (MD) 0007.1 states that 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 information, is not included as IT.

The budget allocation references for TSA's IT assets in the report include the Passenger Screening Program (PSP) and Electronic Baggage Screening Program (EBSP) which comprise the majority of funding activity within the Office of Security Technology, not the Information Technology Division (ITD). This is misleading. The principal function of security screening equipment investments is related to screening persons or items to detect the presence of weapons, prohibited items, and/or explosives. In 2005, TSA captured the IT elements of both PSP and EBSP into a Security Technology Integration Program (STIP) formerly known as the Civilian Aviation Security Screening Network (CASSNET), and all secondary functions falling into the realm of IT in PSP and EBSP investments are effectively managed through STIP. The budget allocated for STIP is nominal when looking at the EBSP and PSP total budgets. The Office of Management and Budget concurs with this assessment and, as recently as March 2007, restated concurrence with the program designations for PSP and EBSP as not including IT and STIP as the screening technology IT program.

The report also states that TSA faces challenges in the areas of meeting stakeholder's diverging interests and accommodating varying stakeholder capabilities, specifically in the area of funding and deploying checked baggage screening systems. TSA actively engages stakeholders on matters of airport checked baggage screening systems. The Baggage Screening Investment Study was undertaken jointly by TSA and aviation industry stakeholders in 2006. As a result of the collaboration of that partnership, draft Planning Guidelines and Design Standards for Checked Baggage Inspection Systems have been developed and are currently under review. We expect the guidelines to be released by the end of calendar year 2007. The design principles and methods presented in the guidelines incorporate insights and experience of industry stakeholders, including airport and airline representatives, planners, architects, baggage handling system designers, and equipment manufacturers. The guidelines will:

- establish common design principles and metrics that all screening system designs shall meet;
- consolidate the collective industry experience and insights on the best practices for planning, designing, and implementing baggage screening systems;
- disseminate the latest information on screening technologies, in-line screening concepts, and screening protocols; and
- standardize the methodology for planning, designing, and evaluating various system design alternatives.

Additionally, in June 2007, TSA issued a guide to airports applying for fiscal year (FY) 2009 EDS Systems and Funding. TSA negotiates agreements with airports called Other Transaction Agreements (OTAs), specifying agreed upon cost-sharing for facility modifications to accommodate optimal in-line EDS solutions. TSA no longer executes multi-year Letters of Intent (LOIs) with airports to fund facility modifications to accommodate in-line EDS solutions. TSA initiated this application guidance to inform airports of the process to follow to apply for OTAs and to collect airport information to use in developing its FY 2009 Spend Plan for EDS. The application process requires airports interested in applying for facility modification funding or requesting equipment to notify their Federal Security Director. The Federal Security Director will convey the airport's interest to TSA headquarters, and shortly thereafter, the airport's designated point of contact will receive the In-line Support Application Form via e-mail. Applying and/or receiving selection notification does not obligate TSA to fund equipment purchase or facility modifications and is subject to annual appropriations levels.

Finally, the report mentions that TSA is challenged with addressing data privacy concerns. Safety and privacy data protections of the new imaging technology were not issues that led to a delay in the field operational test and evaluation. The concern stemmed from discussion of the reaction of the public regarding privacy issues with the images generated by the equipment, not data protection or data privacy issues

Overall, your recommendations will help us continue improving and implementing more effective oversight of IT investments. We concur with your recommendations and have already taken steps to address them. What follows are TSA's specific responses to the recommendations contained in OIG's report.

Recommendation 1: Empowering the Chief Information Officer (CIO) with Agency-wide IT budget and investment review authority to ensure that IT initiatives and decisions support accomplishment of TSA mission objectives.

TSA Concurs: TSA recognizes the need for investment review authority over TSA's IT initiatives. The primary focus has been on ensuring IT resources and purchased services are included in TSA's IT portfolio and support the Agency's strategic business plan, business requirements, and risk management process. TSA is ensuring compliance with DHS MD 0007.1 for CIO accountability of the performance, budgeting, expenditure, and staffing of the Agency's IT resources. TSA is currently reviewing the DHS MD and developing a supplemental TSA MD to delineate roles and responsibilities.

Recommendation 2: Developing a consolidated strategic planning approach to ensure that IT plans across the Agency are well-aligned and linked to the DHS strategic plan, providing a clear vision of how information and technology will be managed to support TSA and DHS mission objectives.

TSA Concurs: In collaboration with the Office of Strategic Planning and Risk Management, ITD is developing the TSA IT Strategic Plan in accordance with the Government Performance and Results Act and the Klinger Cohen Act. This plan outlines TSA's vision, mission, function, strategy, and goals in support of TSA mission objectives through 2010, and incorporates goals

that have been articulated by the Secretary, such as Infrastructure Optimization, Information Sharing and Data Collection, Improved Information Security, and Business Driven IT services. The IT Strategic Plan is scheduled to be circulated for comment in the first quarter of FY 2008.

Recommendation 3: Completing and implementing enterprise architecture to establish technical standards and guidelines for systems acquisitions and investment decisions.

TSA Concurs: TSA recently awarded a contract to provide support for assessing and improving enterprise architecture management. This effort includes mapping processes, organization, data, applications, and infrastructure to the Federal Enterprise Architecture Framework and TSA Strategic Goals. This analysis will help to consolidate common practices, functionalities, and data throughout TSA as well as provide insight in transitioning the TSA Enterprise Architecture from the "As-Is" state to the targeted "To-Be" state. It will also enable the consistent and disciplined use of technology, reduce stovepipe solutions and redundancies, and provide TSA with the capability to plan more efficiently by identifying gaps between the existing and future architectures.

Recommendation 4: Ensuring that the IT services organization establishes and communicates guidelines and procedures for acquiring, developing, and managing IT solutions in a consistent, integrated, and efficient manner.

TSA Concurs: In accordance with DHS MD 0007.1, the TSA Office of the CIO is implementing business processes to ensure the effective management and administration of all Agency IT resources and assets to meet its mission. The TSA investment review process will be centralized within the ITD and will consequently ensure that all programs are assessed in terms of program alignment, enterprise architecture, IT security, and infrastructure and applications optimization. Additionally, MD 300.8, which is posted on TSA's intranet, describes the Investment Review Process, and these items are part of the Program Management certification.

Recommendation 5: Applying adequate staff resources to strengthen the IT Division in addressing IT needs and providing support to TSA operations Agency-wide.

TSA Concurs: The TSA Office of Human Capital completed a position management review for the IT Division on August 15, 2006. The purpose of this review was to identify functions performed, assess assignment of functions to identify any potential duplication, and determine appropriate staffing requirements. The TSA Office of Operational Process and Technology has undertaken an effort to determine the appropriate alignment and full-time equivalent (FTE) allocations for ITD and will be working to ensure appropriate resources are available to carry out this critical Agency mission.

Information Management Division
Sondra McCauley, Director
Kristen Evans, Audit Manager
Steve Ressler, Auditor
Therese Doucet, Auditor
Elizabeth Bakanic, Intern
Beverly Dale, Referencer

Department of Homeland Security
Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
DHS Assistant Secretary for Policy
DHS Assistant Secretary for Public Affairs
DHS Assistant Secretary for Legislative and Intergovernmental Affairs
DHS Chief Information Officer
DHS Deputy Chief Information Officer
Transportation Security Administration Audit Liaison
Assistant Secretary, Transportation Security Administration
Transportation Security Administration, Assistant Administrator, Operational Process and Technology
Transportation Security Administration Deputy Chief Information 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 report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call** our Hotline at 1-800-323-8603;
- **Fax** the complaint directly to us at (202) 254-4292;
- **E-mail** us at DHSOIGHOTLINE@dhs.gov; or
- **Write** to us at:
  DHS Office of Inspector General/MAIL STOP 2600, Attention:
  Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
  Washington, DC 20528,

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