

Department of Homeland Security **Office of Inspector General**

Transportation Security Administration
Has Taken Steps To Address the Insider
Threat But Challenges Remain

(Redacted)



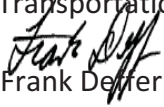
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

September 25, 2012

MEMORANDUM FOR: Dr. Emma Garrison-Alexander
Assistant Administrator for Information Technology
Transportation Security Administration

FROM: 
Frank Deffer
Assistant Inspector General
Information Technology Audits

SUBJECT: *Transportation Security Administration Has Taken Steps
To Address the Insider Threat But Challenges Remain*

Attached for your action is our final report, *Transportation Security Administration Has Taken Steps to Address the Insider Threat But Challenges Remain*. We incorporated the formal comments from the Transportation Security Administration (TSA) in the final report.

The report contains four recommendations aimed at improving TSA's insider threat program. TSA concurred with two recommendations. As prescribed by Department of Homeland Security Directive 077-1, Follow-Up and Resolutions for the Office of Inspector General Report Recommendations, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions at (202) 254-4100, or your staff may contact Richard Saunders, Director, Advanced Technology Division, at (202) 254-5440.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Executive Summary.....	1
Background	2
Results of Audit.....	4
TSA Has Taken Steps To Address the Risk of Insider Threats	4
Challenges Remain in Implementing a Robust Insider Threat Program.....	9
Recommendations	13
Management Comments and OIG Analysis	14

Appendixes

Appendix A: Objectives, Scope, and Methodology	19
Appendix B: Management Comments to the Draft Report	21
Appendix C: TSA’s Layers of Security	27
Appendix D: OIG Assessment of Selected TSA Information Systems.....	31
Appendix E: Major Contributors to This Report	33
Appendix F: Report Distribution	34

Abbreviations

BDO	Behavior Detection Officer
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
FAMS	Federal Air Marshall Service
FBI	Federal Bureau of Investigation
FSD	Federal Security Director
GSS	General Support System
IT	information technology
ITTF	Insider Threat Task Force
JTTF	Joint Terrorism Task Force
MD	management directive
MDVA	Multiple Disciplinary Vulnerability Assessments
NFL	No Fly List
NIST	National Institute of Standards and Technology



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG	Office of Inspector General
OIT	Office of Information Technology
OLE/FAMS	Office of Law Enforcement/Federal Air Marshall Service
OOI	Office of Inspection
SOC	Security Operations Center
TSA	Transportation Security Administration
TSO	Transportation Security Officer
USB	universal serial bus



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Executive Summary

We reviewed the Transportation Security Administration's (TSA's) efforts to address insider threat risks. Our objective was to assess the progress that TSA has made toward protecting its information systems and data from the threat posed by trusted employees. The scope and methodology of this audit are discussed further in appendix A.

TSA has made progress in addressing the information technology insider threat. Specifically, TSA has established an agency wide Insider Threat Working Group and Insider Threat Section responsible for developing an integrated strategy and program to address insider threat risk. Further, TSA is conducting insider threat vulnerability assessments that include personnel, physical, and information systems at selected airports and off site offices. Also, TSA is performing checks on privileged user accounts on TSA unclassified systems. The checks include privileged access accounts and rights granted to system administrators or to other employees whose job duties require specific privileges over an information system or network. Additionally, TSA has established a Security Operations Center responsible for day to day protection of information systems and data that can detect and respond to an insider threat incident.

TSA can further develop its program by implementing insider threat policies and procedures, a risk management plan, and an insider threat specific training and awareness program for all employees. Also, TSA can strengthen its situational awareness security posture by centrally monitoring all information systems and by augmenting current controls to better detect or prevent instances of unauthorized removal or transmission of sensitive information outside of TSA's network boundaries.

We are making four recommendations that, if implemented, would improve TSA's overall management of insider threat risk. TSA concurred with two recommendations and did not concur with two.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. It is responsible for:

- Screening passengers, baggage, and cargo to prevent the smuggling of explosives and other contraband by terrorists and other dangerous suspects;
- Training, monitoring, and certifying Federal flight deck officers, armed security officers, commercial inspectors, and pilot license schools; and
- Leading and conducting security threat assessments and credentialing initiatives for all national modes of transportation, including aviation, maritime, mass transit, highway, freight rail, and pipelines.

TSA relies on sensitive transportation security information to meet these objectives. Every day TSA, airline, and airport vendors or contractors have privileged access to restricted areas that include TSA information systems at the Nation's 459 federalized commercial airports, which could include areas where TSA information systems are being used.¹ As of November 2011, TSA employees consisted of approximately 66,023 Federal employees, of which 51,930 (79 percent) are Transportation Security Officers (TSOs) responsible for screening passengers, carry on baggage, and checked baggage to prevent prohibited objects from being transported on an aircraft.

TSA defines an insider threat as one or more individuals with access or insider knowledge that allows them to exploit the vulnerabilities of the Nation's transportation systems with the intent to cause harm. Types of insider threats could include spying, release of information, sabotage, corruption, impersonation, theft, smuggling, and terrorist attacks. Trusted insiders can be current or former TSA employees, contractors, or partners who have or had authorized access to TSA's operations, systems, and data.

Based on job function or status within the organization, trusted insiders are typically given unfettered or elevated access to mission critical assets, and therefore would be thoroughly familiar with internal policies and procedures, electronic building access systems used for physical security, and technical access controls such as firewalls and intrusion detection systems used for information security. These employees are usually familiar with the weaknesses of organizational policies and procedures, as well as physical and technical vulnerabilities in computer networks and information systems.

¹ Federalized commercial airports operate under TSA-approved security programs.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

This institutional knowledge poses a continual risk to TSA because in the wrong hands it could be used to facilitate malicious attacks and even collusion with external attackers against the organization. The unauthorized disclosure of transportation security information could have an adverse effect on the security of transportation systems, equipment, personnel, or passengers.

TSA currently has multiple layers (i.e., inherent programs or processes) in place that help identify risks to transportation security and could be utilized to mitigate the risks posed by the insider threat. Appendix C lists these layers of security and briefly describes individual security programs.

Since 2001, the Computer Emergency Response Team (CERT) Insider Threat Center of the Software Engineering Institute at Carnegie Mellon University has researched and gathered data about malicious insider acts, including information technology (IT) sabotage, fraud, theft of confidential or proprietary information, espionage, and potential threats to our Nation's critical infrastructures. CERT has researched approximately 400 insider threat cases, including fraud, sabotage, and theft of intellectual property, that have been prosecuted in the United States.

CERT has collaborated with U.S. Secret Service behavioral psychologists to collect approximately 150 actual insider threat cases that occurred in U.S. critical infrastructure sectors between 1996 and 2002, and examined them from both a technical and a behavioral perspective. Their research helped them to develop best practices that provide a framework for establishing an insider threat program within an organization and provide defensive measures that could detect or prevent the insider threat. CERT recommends that organizations:

- Include the insider threat in the enterprise wide risk assessments;
- Conduct a security awareness campaign to ensure that the insider threat is understood across the organization;
- Develop and clearly define policies relevant to the insider threat and enforce these policies consistently and fairly; and
- Secure both the physical and electronic environment, including account and password management, separation of duties, controls for the software development process, change controls, remote access, and privileged user accounts such as those used by system administrators.



Results of Audit

TSA Has Taken Steps To Address the Risk of Insider Threats

TSA has taken a number of steps toward addressing the risk of insider threats to its information systems and data. Specifically, TSA has established an agency wide Insider Threat Working Group and Insider Threat Section responsible for implementing a program to address insider threat risk. In addition, TSA is conducting insider threat vulnerability assessments and checks of privileged user accounts on TSA information systems. Finally, TSA has established a Security Operations Center (SOC) responsible for day to day protection of information systems and data.

Insider Threat Working Group

TSA has established an Insider Threat Working Group, formerly referred to as the Insider Threat Task Force (ITTF), to develop an integrated agency wide strategy that coordinates operational plans to prevent, detect, and deter the exploitation of trusted positions that could jeopardize the security of the Nation's transportation systems.²

In December 2008, TSA decided to examine insider threats issues, and initially tasked the Office of Inspection (OOI) to lead, develop, and facilitate activities for the agency. In early 2009, OOI established the ITTF, which consisted of agency personnel from the various TSA offices, including Chief Counsel, Information Technology, and Security Operations. Its primary goals were as follows:

- To communicate the insider threat program's objectives as they relate to expectations of the current TSA leadership;
- To collaborate agency wide with the implementation of the insider threat program; and

² *Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, issued in 2011, requires agencies that operate or access classified computer networks to implement an insider threat detection program consistent with guidance and standards developed by an interagency, Government-wide insider threat task force. Agencies, such as TSA, will be responsible for implementing an insider threat detection and prevention program consistent with guidance and standards developed by the task force.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- To provide recommendations to TSA leadership on ways to improve the agency's ability to coordinate the ongoing insider threat mitigation efforts.

In 2009, the ITTF proposed a plan to strengthen insider threat mitigation activities. In response to the plan, OOI introduced an Airport Community Engagement Strategy. The strategy included OOI piloting an insider threat awareness campaign and facilitating insider threat Multiple Disciplinary Vulnerability Assessments (MDVAs) at airports on the United States southwest border. The pilots were performed in July 2009. TSA plans to expand the insider threat awareness campaign throughout the TSA workforce.

In January 2012, the ITTF was re established as the Insider Threat Working Group. The working group consists of agency personnel from various TSA offices, including Office of Chief Counsel, Office of Information Technology, and Office of Security Operations.

Insider Threat Section

In January 2011, the leadership of the ITTF was transferred from OOI to the Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS). Additionally, the facilitation of the MDVA and the insider threat awareness briefings were transferred to OLE/FAMS. In March 2011, a permanent Supervisory Air Marshal in Charge was assigned to manage the insider threat program.

The Insider Threat Section, along with the working group, is responsible for:

- Establishing organizational oversight and implementation of an insider threat program;
- Defining, developing, and promoting specific insider threat policies, procedures, and processes to identify, prevent, and detect potential insider threat risks;
- Developing and implementing insider threat reporting and handling requirements for mitigating and responding to insider threat risks, events, or attacks; and
- Developing insider threat requirements for implementing a TSA wide insider threat awareness and training program.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The Insider Threat Section is a central location in TSA for reporting insider threat risks and coordinating insider threat investigations, which may involve TSA offices, external partners, and law enforcement officials. The section evaluates allegations of insider threat incidents, gathers critical information, and preserves evidence.

The section may conduct law enforcement actions to evaluate an allegation of an insider incident, gather critical information, or preserve evidence. It coordinates with the Department of Homeland Security (DHS) Office of Inspector General (OIG), TSA Office of Inspection, the Federal Bureau of Investigation (FBI), or other agencies as necessary to ensure that criminal or administrative allegations are investigated within the appropriate jurisdiction. Insider threat issues that occur at airports are typically reported to the coordinating office by the TSA Assistant Federal Security Director for Law Enforcement.

The section has established a toll free, 24 hour hotline number and an email address specifically for employees and stakeholders to report possible insider threat incidents. It has also developed a brochure and informational poster for employees regarding the Insider Threat Program. The brochure addresses such topics as the motives or personal factors/situations and organizational situations that may increase the likelihood of an insider threat, and behaviors that may offer clues that an employee poses as an insider threat. The informational poster provides basic insider threat indicators and reporting procedures. The brochure and poster are currently pending TSA leadership approval.

Multiple Disciplinary Vulnerability Assessments

The Insider Threat Section performs MDVAs designed to identify and remedy instances that an employee might target with the intent of causing harm from inside the airport environment. The multilayered approach used in the assessments gathers and analyzes identified vulnerabilities from programs or processes that include information systems within the airport security environment. At the end of each assessment, the team suggests countermeasures for improving the airport's insider threat security posture to the Federal Security Director (FSD) and airport authority.³ The methodology used in the insider threat assessment includes:

³ As the highest-ranking TSA employees at federalized airports, FSDs manage Federal airport security staff and operations, and lead and coordinate TSA security activities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Interviewing the FSD, FSD staff, TSOs, and TSA IT specialists assigned to the airport, and airport employees. The interviews are conducted to identify and confirm potential airport insider threat vulnerabilities.
- Performing insider threat technical vulnerability assessments of TSA's IT infrastructure, including networks, servers, and hosts at airports. TSA performs insider threat technical security assessments of the Transportation Security Administration Network General Support System (GSS), Infrastructure Core Services GSS, and End User Computing Major Application.
- Performing insider threat physical security assessments of the entire airport to determine vulnerabilities that could be breached, including locations of TSA's IT infrastructure.
- Performing insider threat analysis obtained during these assessments to identify vulnerabilities an employee could exploit from inside the airport environment. These vulnerabilities could be personnel, physical, or information systems related.

TSA performs these quarterly assessments in collaboration with entities including other TSA internal offices, the FBI, U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, and the Federal Emergency Management Agency. In addition, specific air carriers, airport police, and U.S. Attorney's Office personnel have participated.

Since 2009, 11 MDVAs have been performed. OOI performed eight assessments, including three pilots, and OLE/FAMS performed three assessments.

Technical Insider Threat Vulnerability Assessments

Separate from MDVAs, the Office of Information Technology (OIT) performs technical insider threat vulnerability assessments at selected airports. The assessments are part of a process to specifically address the insider threat from an information security perspective. Since 2011, OIT has performed these assessments at two airports. OIT plans to formalize the assessment process and regularly perform these assessments at selected airports. This assessment methodology includes:

- Conducting interviews at the airport with TSA personnel to determine where potential insider threat issues exist.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Observing and inspecting TSA's operations at the airport, including the screening areas, baggage handling areas, and other TSA areas to identify potential insider threat risks related to information systems.
- Conducting technical vulnerability assessments of TSA's IT infrastructure at the airport and off site administrative offices. The assessments will include TSA's technical infrastructure, servers, and hosts. If identified vulnerabilities require further analysis, TSA will obtain images of the computer hard drives and perform forensic analysis.
- Communicating issues identified during the assessments with the local FSD at the airport to remediate.

Compliance Checks of Information System Privileged Accounts

Employees with privileged access to information systems have a greater opportunity to perform insider attacks, as their elevated user accounts may give them the opportunity to bypass system controls in place to mitigate the insider threat risk.

OIT performs periodic checks of privileged user accounts on selected information systems to verify that policies for secure implementation, monitoring, and maintenance of access controls are properly applied.⁴ These checks are performed under the direction of the TSA Chief Information Security Officer (CISO), and their objective is to determine if selected technical, operational, and management security controls, per *DHS Sensitive Systems Policy Directive 4300A*, are implemented and operating as expected.

As described in TSA's *Standard Operating Procedure (SOP) Privileged Access*, privileged system account holders (e.g., system administrators) are subject to a formal authorization that includes approval by the TSA CISO. By performing these checks, TSA verifies that users who require elevated access to perform their current job functions have been approved.

⁴ TSA defines a privileged account as an information system account with rights that enable a user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

TSA Security Operations Center

Research conducted by CERT has shown that logging and monitoring employees' behavior while they are using Government issued computer or network resources will provide a better opportunity to identify suspicious insider activity before a serious breach of security can occur. TSA's SOC is responsible for day to day monitoring of computer networks and information systems and data. This includes real time analysis of computer system security event logs and computer security incident response as needed.

The SOC collects data and alerts from the following technology assets to determine if insider threat activity is occurring:

- **Firewall Logs** – Reviewing the logs could provide evidence that an insider changed the firewall “rules set” to permit inappropriate activities.
- **Antivirus Logs** – Reviewing the logs could identify an insider who turns off or disables antivirus software, which allows the insider to install malicious files such as viruses, Trojans, or logic bombs.
- **Intrusion Detection System Logs** – Reviewing the logs for network and system activities could identify malicious insider activities or policy violations.

Challenges Remain in Implementing a Robust Insider Threat Program

Although TSA has made progress toward addressing the insider threat risk on many levels, more remains to be done to implement a robust insider threat program. Specifically, TSA can further strengthen its program by implementing specific insider threat policies, procedures, and a risk management plan for the insider threat. TSA needs to implement an insider threat training and awareness program for the entire TSA workforce. Further, TSA should strengthen its situational awareness security posture by centrally monitoring all information systems and by augmenting current controls to detect or prevent instances of unauthorized removal or transmission of sensitive information outside of TSA's network boundaries.

Insider Threat Policies and Procedures

TSA needs to further develop its program by implementing insider threat specific policies and procedures to provide a consistent and clear message to all



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

employees regarding their role and responsibility for mitigating the insider threat risk on a consistent basis. The initial public draft of National Institute of Standards and Technology (NIST) 800 53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommends that an organization develop an insider threat program with clearly defined policies and consistent enforcement of these policies to achieve maximum effectiveness. The Insider Threat Section plans to develop and implement formal insider threat specific policies and procedures that align with existing DHS and TSA policies.

Further, TSA needs to implement a risk management plan specifically addressing the insider threat risk. According to CERT, many organizations that have suffered a loss from an insider threat have done so, at least partially, because of hindrances to effective communication and risk management across departments and their subcomponents. A risk management plan would help ensure that all employees are aware of and addressing risk consistently and continually across the enterprise.

Without insider threat specific policies and an insider threat based risk management plan, there may not be a consistent understanding of the broad spectrum of risks facing TSA.

Insider Threat Specific Training and Awareness Is Needed

TSA does not have an agency wide required training and awareness program that specifically addresses the insider threat. The Insider Threat Working Group is currently identifying insider threat training and awareness needs for all employees, contractors, and Government partners. Once management directives, policies, and standard operating procedures are implemented, TSA plans to create and implement the appropriate insider threat training and awareness activities. The training being developed will include insider threat indicators and processes for reporting suspicious insider threat behavior.

Until insider threat training and awareness for the workforce is implemented, employees, contractors, and partners may not have the knowledge to recognize and help TSA respond to potential insider threats or actual attacks.

Protection of Controlled Information

Protecting controlled information (i.e., sensitive but unclassified or proprietary) is critical to mitigating the insider threat risk to organizations. CERT studied a variety of insider threat cases that revealed circumstances in which insiders



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

carried out attacks through the unauthorized download of information to portable media or external storage devices. In some instances, malicious insiders used email or software protocols to plan their attacks or transmit sensitive or proprietary information to competitors or conspirators.

TSA needs to implement additional protective measures to detect or prevent instances where unauthorized employees using portable media devices (e.g., universal serial buses, or USBs) to copy or remove sensitive data from desktop and laptop computers. According to TSA officials, [REDACTED]

[REDACTED]

[REDACTED]

TSA could implement a variety of monitoring techniques to detect or prevent data loss, including data loss detection tools, enterprise configuration management tools, or host and network based intrusion detection systems. Without these tools, TSA increases the risk of sensitive data being lost, stolen, or destroyed, which could adversely affect TSA property, personnel, or passengers.

Until such tools are utilized across the network enterprise, TSA could implement lesser protective measures to help mitigate this threat. For example, where there is no legitimate “business need” to have USB ports active on desktop or laptop computers, system administrators could disable those ports. Where there is no business need to maintain unlimited file attachment sizes, system administrators could limit the size allowed for file attachments sent via email or transfer protocols, making it more difficult for a malicious insider to exfiltrate large amounts of sensitive data outside of TSA networks without being detected.

Central Monitoring of Information Systems

The SOC currently monitors 60 of 77 unclassified information systems across the TSA enterprise. The remaining systems are monitored either by the system



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

administrator responsible for each system or not at all. Some of these systems are not connected to the TSA network or the Internet.

In 2009, TSA made a risk based decision not to have the SOC monitor the remaining 17 information systems because TSA leadership considered them “non mission critical systems.” However, as part of required security authorization packages, system administrators or owners are required to reassess the *Federal Information Processing Standards 199* security categorization at least every 3 years or when significant changes to the system occur. TSA should reassess the 2009 decision not to monitor these systems based on their perceived low risk categorization.

TSA officials also cited prohibitive cost as a factor in the decision not to extend the monitoring capabilities of the SOC to include these systems. Although TSA has implemented a formal procedure for security breaches on these systems to be reported to the SOC, system administrators tasked to oversee these systems separately may miss an instance of a security breach, because they cannot be expected to review the system’s audit or configuration logs at all times.

According to the *TSA IT Security Handbook*, all information systems security event information is required to be aggregated at a central location. The role of the SOC is to act as a single focal point to provide enhanced situational awareness on IT operational and security issues throughout the enterprise. This positions the SOC to identify, prioritize, and address potential insider threat risks in a timely manner.

Without central monitoring of all information systems, TSA will not have the ability to respond to potential insider threat risks in a timely manner. OIT notified administrators of systems not currently monitored by the SOC that they must either seek an exception to remain that way or arrange to become part of the SOC monitoring. To date, there is no specific timeline to complete this effort.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendations

We recommend that the Assistant Administrator for Information Technology for TSA:

Recommendation #1:

Further develop the insider threat program to include policies, procedures, and a risk management plan pertinent to the insider threat.

Recommendation #2:

Implement an insider threat training and awareness program for the entire TSA workforce.

Recommendation #3:

[REDACTED] direct system administrators to disable USB ports on desktop and laptop computers if there is not a legitimate business need for them to be activated.

Recommendation #4:

Until protective measures are implemented to detect or prevent unauthorized exfiltration of sensitive information outside TSA's network, direct system administrators to limit the size of email file attachments if there is not a legitimate business need for such attachments.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Comments and OIG Analysis

We obtained written comments on a draft report from the TSA Administrator. We have included a copy of the comments, in its entirety, in appendix B. TSA concurred with recommendations #1 and #2 and did not concur with recommendations #3 and #4.

TSA Comments to Recommendation #1

TSA concurs with recommendation #1. TSA stated that it has developed a management directive (MD) that provides TSA policy and procedures for the establishment, integration, and implementation of the Insider Threat Program. The MD is currently in draft pending coordination with other TSA program entities. When approved and implemented, the MD is intended to serve as the foundation for the insider threat specific risk management plan that will identify procedures to use to manage risk throughout the life cycle of an insider threat related activity.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until TSA provides documentation to support that the planned corrective actions are completed.

TSA Comments to Recommendation #2

TSA concurs with recommendation #2. TSA stated that it has an insider threat awareness program, as evidenced by a March 8, 2012, broadcast message entitled *TSA's Insider Threat Program*. The broadcast message defines an insider threat and announced the Insider Threat Program's newly established toll free, 24 hour hotline number, and email address to report possible insider threat incidents.

TSA intends to disseminate and place insider threat posters and tri fold brochures throughout TSA Headquarters and field locations. After the finalization and implementation of the Insider Threat Program MD, TSA will develop insider threat specific training that will likely be delivered to the agency workforce through TSA's Online Learning Center.

The insider threat assessments performed by TSA have recently been enhanced to include insider threat training to FAMS Field Office personnel and individuals



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

that participate in the assessments at the selected airports. The training will include an overview of the Insider Threat Section's roles and responsibilities, as well as the roles and responsibilities of those participating in or supporting the assessments.

OIG Analysis

We agree that the actions being taken satisfy the intent of this recommendation. This recommendation will remain open until TSA provides documentation to support that the planned corrective actions are completed.

TSA Comments to Recommendation #3

TSA did not concur with recommendation #3. TSA stated that it uses USB ports for operational purposes and it would not be feasible to implement the recommendation. [REDACTED]

TSA includes insider threat in its risk based approach to vulnerabilities and views insider threat in every aspect of the TSA mission, including the implementation of protective measures such as physical security, technical controls, and training and awareness. TSA is in the process of creating an Insider Threat Program. TSA OIT has Security Operating Centers that monitor both classified and unclassified systems.

TSA utilizes a gateway application through DHS Trusted Internet Connections and Policy Enforcement Points, which provide alerts when data is transferred outside of the DHS network. TSA continuously works with DHS to fine tune the application for improved notification services within the TSA network. TSA plans to implement policy, procedures, and training to increase awareness, compliance, and accountability among all TSA employees and contractor staff.

OIG Analysis

We consider this recommendation unresolved and will require additional discussion between our offices before disposition. We do not agree with TSA's statement that it uses USB ports for operational purposes and that it would not be feasible to implement the recommendation.

We recognize that TSA has established an agency wide Insider Threat Working Group, Insider Threat Section, and implemented security monitoring at Security



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

information, printing sensitive information, or copying sensitive information by hand.

The TSA strategy for addressing insider threat is a risk based approach that includes the following: an Insider Threat Program, Insider Threat Assessment, Cyber Security Awareness and Outreach Program, Technical Insider Threat Vulnerability Assessment, and compliance checks of information systems privileged accounts.

OIG Analysis

We consider this recommendation unresolved and will require additional discussion between our offices before disposition. We do not consider TSA's comments responsive to the recommendation that email file attachment size should be limited if there is not a legitimate business need for such attachments.

We recognize that TSA has established an Insider Threat Program, conducts insider threat vulnerability assessments, and performs compliance checks of information systems privileged accounts.

[REDACTED]

As discussed with TSA, this recommendation was meant to serve as a lesser and interim protective measure until TSA has implemented the appropriate protective measures.

DHS MD 4500.1, *DHS E Mail Usage*, gives email system administrators the responsibility for implementing and maintaining appropriate security features and controls. Although DHS users are responsible for adhering to the CIO's guidelines on email message size, only administrators at the direct system level have both the control and responsibility to address the security risk posed by exfiltration of sensitive information. Furthermore, administrators can impose email size limitations based on the specific and unique needs of user roles and accounts. For example, 79 percent of TSA's workforce are TSOs, who have a minimal need to attach sensitive information to email files on a daily basis.

Implementing different, but appropriate security schemes and settings to the email accounts based on business needs, is a crucial step for TSA to limit its exposure to potential insider threat risks. TSA should reconsider its response to



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

this recommendation and take the necessary steps to address this potential insider threat risk.



Appendix A

Objectives, Scope, and Methodology

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.

The objective of this audit was to assess the progress that TSA has made toward protecting its information systems and data from the threat posed by trusted employees.

During the audit, we assessed TSA's:

- Insider threat management process;
- Ability of selected employees to monitor and report suspicious employee behavior;
- Insider threat security policies;
- Insider threat security training and awareness; and
- Four unclassified information systems critical to the mission of TSA.

Appendix D provides information on the systems selected for the assessment, relevant security controls selected, and the assessment results.

Fieldwork was conducted at:

- TSA Headquarters, Arlington, Virginia;
- Denver International Airport, Denver, Colorado;
- Colorado Springs Airport, Colorado Springs, Colorado;
- Washington Dulles International Airport, Sterling, Virginia;
- Charlotte Douglas International Airport, Charlotte, North Carolina;
- Raleigh Durham International Airport, Morrisville, North Carolina;
- Ronald Reagan Washington National Airport, Arlington, Virginia;
- Colorado Springs Operations Center;
- Annapolis Junction Operations Center;
- TSA Security Operations Center, Ashburn, Virginia;
- TSA Freedom Center, Herndon, Virginia;
- Federal Air Marshal Service Facility, Egg Harbor Township, New Jersey; and
- DHS Data Center, Clarksville, Virginia.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Fieldwork was performed through conference calls or data calls for the San Francisco International Airport in San Francisco, California, and the Portland International Airport in Portland, Oregon.

We conducted this performance audit between September 2011 and March 2012 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate TSA's efforts to provide the necessary information and access to accomplish this audit. Major OIG contributors are identified in appendix E.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Report



JUN 25 2012


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



Transportation
Security
Administration

INFORMATION

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General
Information Technology Audits

FROM: John S. Pistole 
Administrator

SUBJECT: Transportation Security Administration's (TSA) Response to
Department of Homeland Security (DHS) Office of Inspector
General's (OIG) Draft Report Titled *Transportation Security
Administration Has Taken Steps To Address the Insider Threat But
Challenges Remain*, OIG Project No. 11-064-ITA-TSA

Purpose

This memorandum constitutes TSA's formal Agency response to the DHS OIG draft report *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain*. TSA appreciates the opportunity to review and provide comments to your draft report.

Background

In August 2011, OIG began a review of TSA's efforts to address insider threat risks. OIG's objective was to assess the progress that TSA made toward protecting its information systems and data from the threat posed by trusted employees. OIG conducted its fieldwork from September 2011 to March 2012.

During this review, OIG assessed TSA's insider threat management process; ability of selected employees to monitor and report suspicious employee behavior; insider threat security policies; insider threat security training and awareness; and four unclassified information systems critical to the mission of TSA.





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

[REDACTED]

2

Discussion

As noted in the draft report, OIG's objective was to "assess the progress that TSA has made toward protecting its information systems and data from the threat posed by trusted employees." DHS OIG noted that TSA has made progress in addressing the information technology insider threat. Specifically, the report states that "TSA established an agency-wide Insider Threat Working Group and Coordinating Office responsible for developing an integrated strategy and program to address insider threat risk." TSA appreciates OIG's recognition of TSA's efforts to address insider threat risks by conducting insider threat vulnerability assessments that include personnel, physical, and information systems at selected airports and off-site offices; performing checks on privileged user accounts on TSA unclassified systems (which include privileged access accounts and rights granted to system administrators or to other employees whose job duties require specific privileges over an information system or network); and establishing a Security Operations Center responsible for the day-to-day protection of information systems and data that can detect and respond to an insider threat incident.

There are several items contained in the report TSA would like to clarify. In reference to the definition of insider threat, TSA seeks to clarify that it defines an insider threat as "One or more individuals with access and/or insider knowledge that allows them to exploit the vulnerabilities of the Nation's transportation systems with the intent to cause harm. This includes direct risks associated with TSA's security programs, operations, and indirect risks that may compromise our critical infrastructure." The referenced definition was disseminated to the entire TSA workforce through a TSA broadcast message on March 8, 2012, as part of TSA's Insider Threat Program awareness campaign.

With respect to steps TSA has taken to address the risk of insider threats, specifically as it concerns the Insider Threat Working Group (ITWG) and the Insider Threat Section, TSA seeks to clarify, for historical accuracy, the evolution of these entities and associated nomenclatures. In December 2008, TSA's Office of Inspection (OOI) was tasked by TSA leadership to lead and/or coordinate the Agency's insider threat initiatives, to eventually include the Insider Threat Task Force (ITTF), which was re-established in January 2012 as the Insider Threat Working Group (ITWG). Similar to the ITTF, the ITWG consists of Agency personnel from various TSA offices, including the Office of Chief Counsel, Office of Information Technology, and Office of Security Operations.

In response to the ITTF's proposed plan to strengthen insider threat mitigation activities, in 2009, OOI introduced an Airport Community Engagement Strategy (ACES). The strategy included OOI piloting an insider threat awareness campaign and facilitating insider threat Multiple Disciplinary Vulnerability Assessments (MDVAs) at airports on the United States southwest border.

One of the ITTF's recommendations to TSA leadership was to establish an insider threat coordination office that would be responsible for coordinating TSA's insider threat program efforts. In January 2011, in response to this recommendation, TSA established the Insider Threat

[REDACTED]



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

3

Section within TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS). The Insider Threat Section is responsible for the ITWG (formerly the ITTF), as well as facilitation of the MDVA and insider threat awareness briefings.

The purpose for and primary goals of the ITWG are consistent with those of the ITTF; however, the Insider Threat Section, along with the working group, is also responsible for the following:

- Establishing organizational oversight of an insider threat program;
- Defining, developing, and promoting specific insider threat policies, procedures, and processes to identify, prevent, and detect potential insider threat risks;
- Developing and implementing insider threat reporting and handling requirements for mitigating and responding to insider threat risks, events, or attacks; and
- Developing insider threat requirements for implementing a TSA-wide insider threat awareness and training program.

The Insider Threat Section's coordination with other DHS or TSA offices, and/or other agencies, is not strictly limited to the investigation of criminal allegations. Coordination may also occur pursuant to an investigation of administrative allegations. Additionally, under the current model, the Insider Threat Section oversees the following three functional areas or program sections:

- Insider Threat Assessments (ITAs)
- Training and Awareness
- Operations: Referrals and Mitigation.

With respect to the number of MDVAs performed by TSA, since 2009 it has conducted 11, as opposed to five as indicated in the report. OOI facilitated eight MDVAs, including three pilots; and to date, OLE/FAMS has facilitated three MDVAs.

Statements within the report portray an absence of any insider threat education, training, and awareness at TSA. Although TSA does not have an Agency-wide required training and awareness program that specifically addresses insider threat, it has mandatory Online Learning Center courses that include aspects of awareness and recognition of insider threat activities, e.g., *TSA Security Orientation*, *Classified National Security Information (CNSI) for TSA Employees and Contractors*, *Fundamentals of CNSI*, *Operations Security Fundamentals (OPSEC)*, *IT Security Awareness*, and *TSA Management Directive (MD) 2800.5: Internal Security Reporting: Foreign Contact and Travel*. Over the years, awareness programs have been deployed within TSA that address being alert to external influences and co-worker criminal and intelligence involvement, programs that have included poster campaigns at Headquarters and field offices, broadcast messages, and OPSEC or Sensitive Security Information survey visits at major airport



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

4

offices. While TSA agrees that such efforts are shared among the multiple TSA program offices, and not presently issued under one consolidated program, they are representative of the supporting efforts by program offices within TSA to raise awareness of insider threat.

Overall, your recommendations will help us continue improving and implementing a more robust insider threat program. TSA has already made significant progress in implementing a more robust insider threat program, as evidenced by the fact that when audit fieldwork began, the Insider Threat Section was only staffed with the Supervisory Air Marshal in Charge. At present, the Insider Threat Section currently consists of 10 full-time employees. Additionally, a program specific TSA Management Directive (MD) and Concept of Operations (CONOPS), as well as an informational poster and tri-fold brochure, have been developed and are currently pending leadership approval. Further, a toll-free, 24-hour hotline number and e-mail address have been established specifically for use by employees and stakeholders to report possible insider threat incidents, reporting methodologies recently disseminated, along with a definition of an insider threat, to the TSA workforce on March 8, 2012. TSA recognizes the threat posed by the unauthorized removal, copying, or dissemination of sensitive information and has implemented a spectrum of protective measures to address these risks, including physical security, technical controls, and employee training.

What follows are TSA's specific responses to the recommendations contained in OIG's report.

Recommendation 1: Further develop the insider threat program to include policies, procedures, and a risk management plan pertinent to the insider threat.

TSA Concurs: TSA has developed a MD that provides TSA policy and procedures for the establishment, integration, and implementation of the Insider Threat Program. The MD is currently in draft pending coordination with other TSA program entities. Several of the procedures accompanying the MD are derived from a CONOPS, which is also currently in draft pending leadership approval.

The implementation of the referenced documents is intended to serve as the foundation for the Insider Threat Program's multi-faceted, insider threat specific risk management plan, which will identify procedures to be used to manage risk throughout the life-cycle of an insider threat related activity. Additionally, it will identify procedures for performing risk identification and quantification, planning risk response, implementing contingency plans, allocating reserves and documenting results.

Recommendation 2: Implement an insider threat training and awareness program for the entire TSA workforce.

TSA Concurs: TSA has an insider threat awareness program evidenced by a March 8, 2012 broadcast message entitled, *TSA's Insider Threat Program*, that defined an insider threat and announced the Insider Threat Program's newly established toll-free, 24-hour hotline number and e-mail address to report possible insider threat incidents. Pending are posters and tri-fold



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

5

brochures intended for dissemination to and placement throughout TSA Headquarters and field locations. TSA will develop insider threat specific training upon finalization and implementation of the Insider Threat Program MD. Delivery of the training to the Agency workforce will likely be through TSA's Online Learning Center. ITAs have recently been enhanced to include insider threat training to FAMS Field Office personnel, individuals that will participate in the ITA activities at the ITA selected airports. The training involves an overview of the Insider Threat Section's roles and responsibilities, as well as roles and responsibilities of those participating in and/or supporting the assessment. These methodologies for raising awareness, coupled with the Insider Threat MD and accompanying procedures, will equip the workforce with the ability to recognize and to appropriately respond to a potential or actual insider threat attack.

Recommendation 3:

direct system administrators should disable USB ports on desktop and laptop computers if there is not a legitimate business need for them to be activated.

TSA Non-Concurs: TSA uses USB ports for operational purposes. Therefore, implementation of the recommendation is not feasible. TSA intends to implement peripheral device mitigating solutions through software in future security solution upgrades. TSA includes insider threat in its risk-based approach to vulnerabilities. TSA views insider threat in every aspect of the TSA mission to include the implementation of protective measures ranging from physical security, technical controls, training and awareness, and the stand up of an Insider Threat Program. Moreover, TSA OIT has specific Security Operating Centers (SOCs) that monitor both classified and unclassified systems. TSA utilizes a gateway application through DHS TIC and PEP, which provide alerts when data is transferred outside of the DHS network. TSA continuously works with DHS to fine-tune the application for improved notification services within the TSA network. TSA plans to implement policy, procedures, and training to increase awareness, compliance and accountability among all TSA employees and contractor staff.

Recommendation 4: Until protective measures are implemented to detect or prevent unauthorized exfiltration of sensitive information outside TSA's network, direct system administrators should limit the size of email file attachments if there is not a legitimate business need for such attachments.

TSA Non-Concurs: TSA physical and automated security controls prevent inadvertent access to sensitive data and uses role based scenarios and periodic review of all security controls prior to receiving an approval to operate those systems where sensitive data is housed. NIST 800.45 recommends that organizations should consider restricting the maximum applicable size for e-mail attachments. Additionally, DHS MD 4500.1 gives the Chief Information Officer (CIO) the responsibility for establishing individual mail message size (including attachments) and total mailbox size limits. Accordingly, TSA currently limits the size of e-mail attachments to 20MG for all employees. However, imposing e-mail size limitations will not inhibit the ability of "insiders" to copy or disseminate sensitive information. TSA recognizes that sensitive information can be copied or disseminated through various methods, including, but not limited



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

[REDACTED]

6

to: sending multiple e-mail attachments, sending e-mails with embedded sensitive information, printing sensitive information, or copying sensitive information by hand. The TSA strategy for addressing insider threat is a risk-based approach that includes the following: an Insider Threat Program, Insider Threat Assessment, Cyber Security Awareness and Outreach Program, Technical Insider Threat Vulnerability Assessment, and compliance checks of information systems privileged accounts.



Appendix C

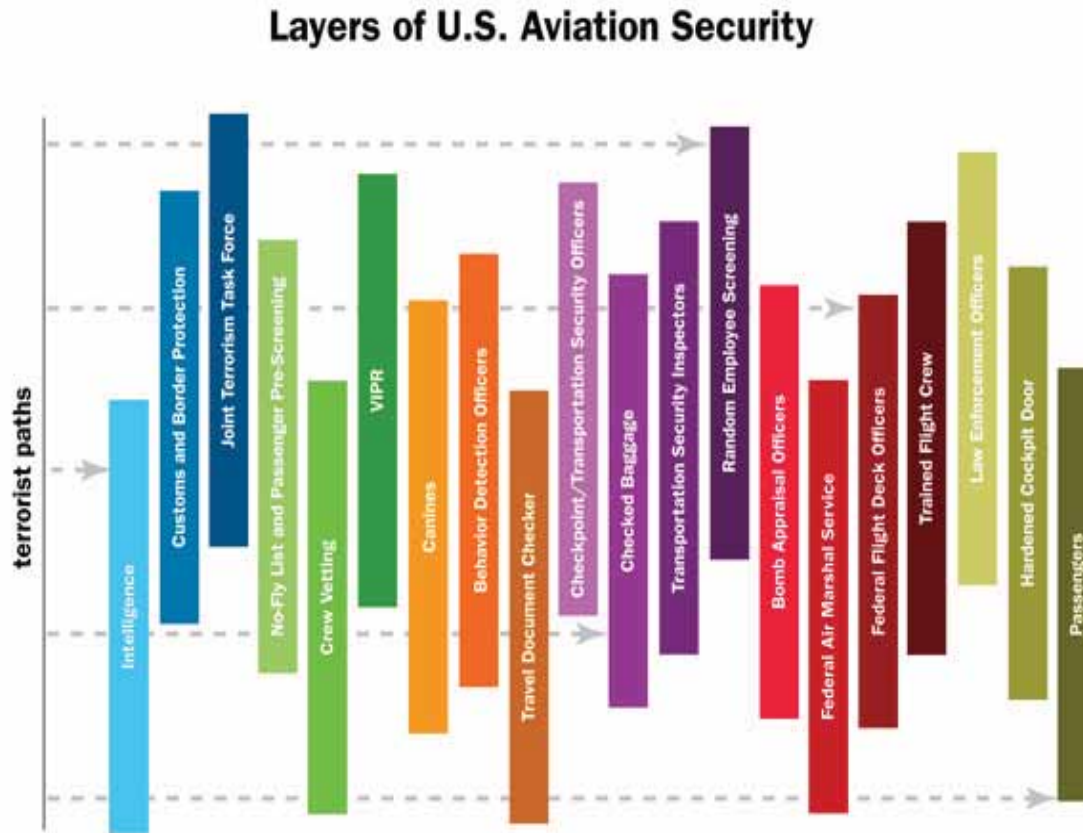
TSA's Layers of Security

TSA has multiple layers of aviation security that could mitigate the risk of insider threat through individual TSA security programs. These layers of security are designed to deter individuals attempting to carry out terrorist attacks. Figure 1 shows TSA's 20 layers of aviation security.

The security layers and the processes they establish could identify risks to aviation security, which could include the insider threat. These security layers include using airport checkpoints, gathering and analyzing intelligence, checking passenger manifests against watch lists, performing random canine searches at airports, and employing Federal flight deck officers and Federal air marshals. These areas are not discussed in the body of the report.



Figure 1: TSA's 20 Layers of Aviation Security



Source: TSA

According to TSA, each layer has the potential to prevent a terrorist attack; together, the layers create a much stronger security system. Potential terrorists would have to overcome multiple layers to carry out an attack and would most likely fail in their attempts.

Insider threat related activities are integrated into the security layers. Listed below are individual TSA security programs that could help mitigate the insider threat.

Personnel Background Investigations and Vetting

TSA requires all employees and contractors to undergo a background investigation prior to employment. To gain privileged access to secure areas of federalized airports, TSA, airline, airport, and airport vendor employees and contractors must possess a Security Identification Display Area badge granted by the airport authority. Before issuing an identification badge, the airport authority performs a criminal history record check on each individual who needs access. The airport authority provides this information to



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

TSA, and it is vetted for known threats to transportation or national security. TSA then compares those results to a list of disqualifying offenses.⁵ If applicants have been convicted in the past 10 years of any of the offenses, they are prohibited from employment.

Daily, TSA performs perpetual name based vetting of all TSA, airline, airport, and airport vendor employees and contractors. TSA compares the names against various law enforcement and intelligence agency databases to determine whether there is a potential or actual threat to transportation security. If TSA determines that an individual poses a security threat, the information is sent to the appropriate law enforcement or intelligence agencies for further analysis.

The law enforcement or intelligence agencies determine whether the individual's identity can be verified and whether the individual continues to pose a threat or is suspected of posing a threat, and notifies TSA. TSA informs airlines or airports when an individual's access to secure areas must be denied or rescinded.

Airport Security Playbook Program

TSA's Airport Security Playbook program uses security countermeasures designed to detect, deter, and defeat potential insider actions within the Nation's aviation system. Beginning in 2008, the program was deployed at federalized airports to improve the overall security posture among the airports.

The playbook includes a predefined list of plays, actions, and scenarios that the Federal Security Director Playbook Coordinator executes on a daily basis in coordination with TSA personnel, local law enforcement, and other DHS agencies at the airport. The program creates a dynamic security environment that increases unpredictability, which is designed to frustrate potential terrorist plans or activities.

Behavior Detection Officer Program

TSA established the Behavior Detection Officer (BDO) program to use nonintrusive behavior and analysis techniques to identify potentially high risk passengers and employees. BDOs are trained to detect individuals exhibiting behaviors that indicate they may be a threat to transportation security. BDOs are currently operating at approximately 161 airports nationwide.

⁵ See 49 USC 44936(b) and 49 CFR 1542.209(d) for lists of disqualifying offenses.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Joint Vulnerability Assessments by TSA and the FBI

TSA and the FBI perform congressionally mandated, periodic joint vulnerability assessments of security at selected airports to assess current and potential threats to the domestic air transportation system. The assessments consider the extent of individuals' capability and intent to carry out terrorist attacks or related actions against transportation systems and how those individuals might carry out those actions.

Joint Terrorism Task Forces

TSA participates in Joint Terrorism Task Forces (JTTFs). JTTFs provide a central location for local, State, and Federal agencies to share terrorism related information and intelligence and to investigate terrorist threats, including insider threats. TSA regularly participates in FBI led JTTFs throughout the United States, including the National JTTF.

TSA's Office of Inspection

TSA's Office of Inspection performs a variety of activities related to identifying and investigating threats, such as conducting inspections; performing covert testing; conducting criminal and administrative investigations of employees; and identifying and testing vulnerabilities in passenger, baggage, and cargo operations.



Appendix D

OIG Assessment of Selected TSA Information Systems

Our review of four unclassified information systems critical to the TSA mission and the safety of airline employees, passengers, and the general public included the following:

- Crew Vetting Program – Used by TSA to conduct security threat assessments of airline crew members.
- Mission Scheduler Notification System – Provides TSA with automated means for mission planning and scheduling for the FAMS.
- No Fly List (NFL) HTML Database – Provides TSA, airline carriers, embassies, and other Federal agencies with a current list of individuals who may pose a threat to aviation security, airline carriers, embassies, and other Government agencies. The NFL is created and maintained by the FBI’s Terrorist Screening Center and provides a consolidated list of known or suspected terrorists.
- Transportation Worker Identification System – Provides identity credentials for transportation workers who require unescorted access to secure areas of the Nation’s transportation infrastructure.

Minimum Technical and Physical Security Controls on Information Systems Are Present

Our review of the technical and physical controls concludes that TSA has applied the minimum required security controls designed to provide reasonable assurance that information systems audited are protected against vulnerabilities that are commonly exploited by attackers.⁶

⁶ The DHS 4300A and NIST Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* based controls reviewed included the following: Account Management (AC-2), Separate of Duties (AC-5), Least Privilege (AC-6), Remote Access (AC-17), Audit Review, Analysis, and Reporting (AU-6), Access Restrictions for Change (CM-5), Risk Assessment (RA-3), Physical Environment Protection Policy and Procedures (PE-1), Physical Access Authorizations (PE-2), Physical Access Control (PE-3), Monitoring Physical Access (PE-6), and Visitor Control (PE-7).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Minimum Technical Security Controls Applied⁷

- TSA has defined processes for creating and deleting information system user accounts.
- TSA reviews and analyzes information system audit logs for indications of inappropriate or unusual activity and reports findings to the appropriate officials for further action or instruction.
- Remote access to information systems is restricted to authorized personnel and requires strong authentication accomplished through two factor authentication to access the system.
- Separation of duties is enforced. Users are assigned duties based on position to prevent one person from having full access to the system in all process activities.

Minimum Physical Security Controls Applied⁸

- Policies and procedures are documented in *TSA's IT Security Policy Handbook* (see chapter 3) for implementation guidance for physical and environmental protection of the information system facilities. TSA policies are reviewed and updated annually by the TSA Infrastructure Assurance and Cyber Security Division, Information Assurance Policy Branch.
- TSA develops and keeps a current list of authorized personnel who have access to the information system facilities. The lists are regularly updated as personnel are added and removed based on hiring, separation, and change in job duties.
- Buildings and rooms housing information systems, equipment, and data are monitored by real time intrusion alarms and surveillance equipment to detect and respond to physical security incidents.
- TSA requires visitors to sign in upon entering information system facilities, be escorted during their stay, and sign out upon leaving the facility. Visitor logs are maintained and available for review for 1 year.

⁷ According to NIST Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, technical controls provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

⁸ According to NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, physical security controls are part of the physical and environmental protection control family.



Appendix E

Major Contributors to This Report

Richard Saunders, Director
Philip Greene, Audit Manager
Jason Dominguez, Management Analyst
Jamie Horvath, IT Specialist
Sandra Ho, IT Specialist
Scott He, IT Specialist
Michael Horton III, Management and Program Assistant
Kelly Herberger, Communications Analyst
Craig Adelman, Referencer



Appendix F

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Respective Under Secretary
Director of Local Affairs, Office of Intergovernmental Affairs
Chief Information Officer
Chief Information Security Officer

Transportation Security Administration

TSA Administrator
TSA Deputy Administrator
TSA Chief Information Officer
TSA Chief Information Security Officer
TSA Audit Liaison
FAMS Chief, IT Security
FAMS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

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

For additional information, visit our website at: www.oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

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

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

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