Department of Homeland Security
Office of Inspector General

Transportation Security Administration Privacy Stewardship

OIG-09-97

August 2009

Office of Inspector General

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

Homeland Security

August 28, 2009

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 the Transportation Security Administration's plans and activities to instill and promote an effective culture of privacy in compliance with federal privacy laws and regulations. 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. We trust 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

Figures

Appendices

Abbreviations

DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
FIPPs	Fair Information Practice Principles

Table of Contents/Abbreviations

FISMA	Federal Information Security Management Act
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPPC	Transportation Security Administration, Office of Privacy Policy and Compliance
PII	personally identifiable information
PIA	Privacy Impact Assessment
PTA	Privacy Threshold Analysis
SORN	System of Records Notice
TSA	Transportation Security Administration

Executive Summary

We performed an audit of the Transportation Security Administration's (TSA) privacy stewardship. Our audit objective was to determine whether TSA's plans and activities instill and promote a privacy culture and comply with federal privacy laws and regulations. As part of this audit, we surveyed 2,285 TSA employees on their knowledge of the *Privacy Act*, the proper handling of personally identifiable information, privacy incident response, and privacy stewardship. The results of this survey are discussed throughout the report. Appendix A provides our purpose, scope, and methodology.

TSA has made progress in implementing a framework that promotes a privacy culture and complies with federal privacy laws and regulations. Specifically, TSA demonstrated its organizational commitment to privacy by designating the Office of Privacy Policy and Compliance (OPPC) to oversee its privacy functions. In addition, OPPC is strengthening TSA's culture of privacy through coordination with managers of programs and systems that contain personally identifiable information to meet reporting requirements, perform privacy risk impact assessments, prepare public notifications of systems of records, and enforce privacy rules of conduct. Further, OPPC has established processes for reviewing and reporting privacy incidents, issuing public notices, addressing complaints and redress for individuals, and implementing and monitoring privacy training for employees.

TSA can improve its privacy program by implementing automated privacy-specific tools for testing and monitoring. Further, TSA can implement approaches to provide supplemental and job-specific privacy awareness or training activities. We are making two recommendations to the TSA Administrator to strengthen the privacy program.

Background

The *Privacy Act of 1974*, as amended, imposes various requirements on agencies whenever they collect, use, or disseminate personally identifiable information (PII). Additionally, federal laws, regulations, directives, and guidelines set the minimum standards and procedures for handling PII. Appendix H lists some requirements specific to TSA privacy stewardship.

TSA facilitates the security and freedom of movement of the nation's air, surface, and maritime transportation systems. This requires coordinating or overseeing the security of highways, buses, mass transit systems, railroads, pipelines, ports, and approximately 450 U.S. airports. More than 40,000 TSA employees stationed throughout the world interact daily with the public or collect, use, and disseminate PII about the public. In 2009, for example, TSA implemented the Secure Flight program which will eventually require a substantial volume of PII to screen airline passengers. According to the U.S. Department of Transportation's Bureau of Transportation Statistics, U.S. airlines carried 649.9 million domestic passengers on 9.3 million flights in 2008.

TSA defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is or can be linked to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the United States. Figure 1 shows the purposes for which TSA collects PII for 10 TSA programs that we reviewed during this audit.

TSA's PURPOSES FOR PERSONALLY IDENTIFIABLE INFORMATION
Examples
THREAT ASSESSMENT & CREDENTIALING
▪ Perform security threat assessments: alien flight students; airline crew members; aviation travelers; hazardous material drivers ▪ Confirm identity of national transportation system workers via biometric credential ▪ Screen cargo transported by passenger aircraft
LAW ENFORCEMENT
▪ Protect flight deck against acts of criminal violence or air piracy ▪ Share transportation security intelligence with federal, state, and local law enforcement
REDRESS
▪ Provide a one-stop mechanism for individual redress

Figure 1. TSA's Purposes for Personally Identifiable Information
Source: OIG Analysis of Privacy Impact Assessments and System of Records Notices for 10 PII programs. (See appendix C for details on these programs.)

The Department of Homeland Security (DHS) Privacy Office promotes the growth of privacy programs within the DHS components as a means of addressing privacy. Further, the DHS Privacy Office is implementing a privacy framework that establishes the roles and responsibilities for component privacy offices. Figure 2 illustrates the DHS privacy framework.

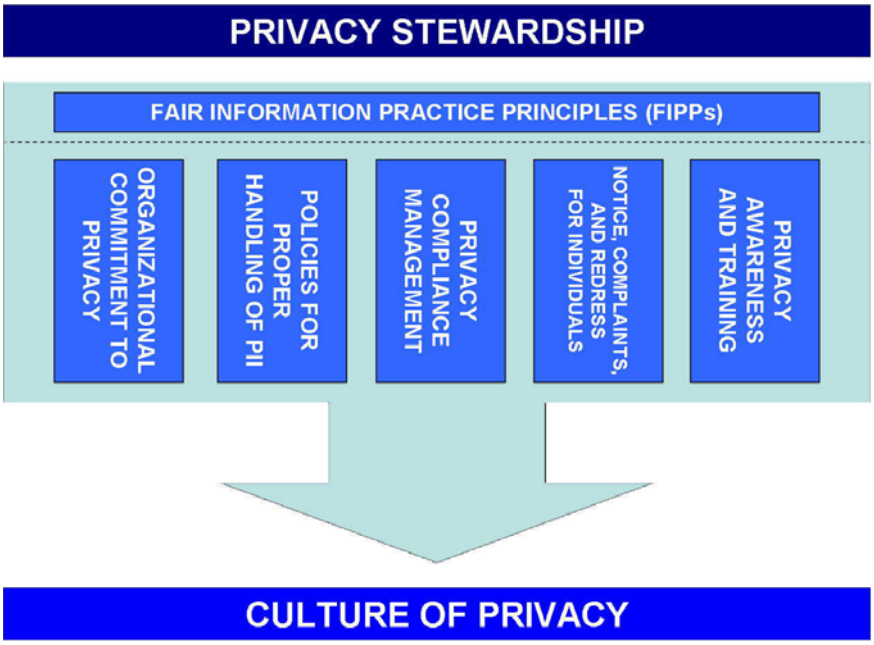


Figure 2. DHS Privacy Framework
Source: DHS Privacy Office

Privacy stewardship includes establishing privacy requirements prior to program initiation, performing privacy risk assessments and mitigation, and integrating privacy safeguards into program operations. Responsible stewardship of PII through each of the functional areas of an agency privacy program is fundamental to instilling a culture of privacy.[1] Promotion of an effective culture of privacy leads to embedded shared attitudes, values, goals, and practices for complying with the proper handling of PII and the recognition that the public and employees should have protections of how their PII is used.

The Fair Information Practice Principles (FIPPs) are a set of principles, rooted in the tenets of the *Privacy Act*, that form the basis of TSA's privacy compliance policies and procedures for

[1] A privacy program is a comprehensive approach to managing privacy compliance and risk in DHS programs and activities. (Adapted from NIST Special Publication 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.)

governing the use of PII.[2] Also part of the privacy framework are five functional areas that promote a culture of privacy and compliance with legal requirements. (See appendix D for component privacy officer duties and appendix E for legal requirements, including TSA directives, that relate to these functional areas.)

- **Organizational Commitment to Privacy:** Establish organizational oversight and implement privacy activities.
- **Policies for Proper Handling of PII:** Define and promote privacy policies and procedures.
- **Privacy Compliance Management:** Implement tools and processes to ensure privacy compliance (including reporting requirements, privacy impact assessments, systems of records notices, privacy incident handling, and privacy rules of conduct).
- **Notice, Complaints, and Redress for Individuals:** Establish processes for notices, complaints, and redress for individuals.
- **Privacy Awareness and Training:** Support privacy requirements through privacy awareness and training.

[2] DHS Privacy Office, *Privacy Policy Guidance Memorandum 2008-01*, December 29, 2008, adopted the Fair Information Practice Principles as its privacy policy framework for application by DHS programs and activities. (See appendix F for descriptions of each of the principles.)

Results of Audit

Commitment to Privacy

TSA has an organizational commitment to privacy stewardship. Figure 3 illustrates three factors indicating TSA's commitment to privacy that include the designation of a privacy point of contact for oversight, development of internal privacy stewards, and managers promoting privacy compliance.

Figure 3. Organizational Commitment to Privacy
Source: OIG analysis from TSA documentation.

Designation of a Privacy Point of Contact

In 2004, confronted with privacy challenges from collecting large volumes of PII, TSA appointed a privacy officer to address privacy issues and issued guidance to employees and managers regarding their responsibility to respect and protect privacy. The goals were to instill and promote a culture of privacy throughout TSA's operations, and to protect and respect the privacy of individuals affected by TSA's transportation activities.

In 2006, TSA designated the director of the Office of Privacy Policy and Compliance (OPPC) to assume TSA's privacy function. To assist in creating a privacy program, TSA added two staff with privacy-related experience and certifications to OPPC. TSA also added a program-level privacy contact for Secure Flight and embedded four privacy specialists into its operation.

OPPC coordinates and oversees privacy protections according to TSA Management Directive 2100.2, *Privacy and Information Collection Policy*, by taking a service-oriented approach to working with TSA personnel and setting a goal to acknowledge inquiries within 24 hours. As a measure of OPPC's outreach, 92% of surveyed employees indicated that they are aware of OPPC's presence and roles; 82% of surveyed employees consider privacy to be important.

Also, OPPC reaches out to external groups to gather information, improves agency visibility as a privacy leader, and promotes organizational involvement in privacy efforts, participation on privacy-related boards, presentations at conferences, and sharing of best practices. Further, OPPC participates on the DHS Privacy Office's committees, such as DHS best practices and privacy contract clauses.

Development of Internal Privacy Stewards

OPPC is responsible for monitoring TSA compliance with privacy law and instilling a culture of privacy. However, since OPPC has a small staff, developing privacy stewards within TSA can multiply the effectiveness of OPPC's privacy awareness and outreach. Privacy stewards are individuals outside OPPC who promote compliance with privacy requirements and support a culture of privacy at job-specific levels. Progress has been made in developing privacy stewards by implementing privacy awareness activities and reaching groups within TSA; 45% of surveyed employees consider themselves privacy stewards.

Working with internal groups is one way OPPC promotes the concept that everyone in TSA is responsible for privacy. OPPC participates in various meetings and integrated program teams and provides guidance on the privacy implications and interpretation of privacy criteria. Program and security managers told us that they regularly contact OPPC for privacy assistance and guidance.

OPPC interacts with privacy stewards to gain a better understanding of privacy risk in mission-related programs and how these risks relate to the overall level of TSA's commitment to privacy. The development of an organization-wide cadre of privacy stewards is important in helping employees who handle PII to understand that PII is a critical data asset that must be fully aligned with program objectives.

Managers Promoting Privacy

Managers promote privacy to ensure that anyone entrusted with PII properly uses, protects, and disposes of PII. TSA program managers and supervisors take a proactive approach to privacy stewardship. For example, some program managers maintain standard operating procedures on employing proper PII handling. In compliance with TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information*, supervisors remind employees about proper PII handling and hold themselves and their workforce accountable.

Policies on the Proper Handling of Personally Identifiable Information

As required by TSA Management Directive 3700.4, OPPC issues policies and procedures to define privacy compliance and promote its overall privacy mission. Management communicates its views and requirements to employees through internal privacy policies and procedures. OPPC publishes these privacy policies and guidance on its intranet site. Almost 75% of surveyed employees who collect, handle, view, or maintain PII said that they look for privacy policies and procedures on the intranet privacy website.

OPPC issued TSA Management Directive 3700.4 to describe privacy requirements and provide examples of what would be considered privacy incidents. OPPC's guidance on privacy incident reporting is consistent with Office of Management and Budget (OMB) and DHS Privacy Office requirements. Almost 80% of surveyed employees were able to identify a privacy incident correctly from a list of five examples. Nearly 95% of surveyed employees said that they knew the reporting procedures for suspected privacy incidents.

TSA Management Directive 3700.4 also explains how employees can implement methods for handling sensitive PII and requires TSA employees to review their responsibilities annually to comply with the *Privacy Act* and DHS and TSA privacy policies. Almost 80% of surveyed employees demonstrated knowledge by correctly identifying the requirements of the *Privacy Act* and TSA privacy policies.

DHS 4300A, *Sensitive Systems Handbook*, requires TSA to provide a security and privacy statement at every publicly accessible electronic entry point and display a warning banner on its intranet. TSA has external privacy notices and internal network banners to provide pertinent information to the public and to remind employees of the importance of their responsibilities for privacy compliance. OPPC reviews these statements and banners for compliance with privacy requirements.

Compliance With Federal Privacy Laws and Regulations

TSA Management Directive 2100.2 establishes OPPC's responsibility for an internal privacy management program to ensure that all PII gathered under the *Privacy Act* is handled properly. OPPC executes plans and activities to comply with federal privacy laws, directives, and the FIPPs. For example, OPPC assists TSA program managers in integrating FIPPs into their programs that require PII.

Figure 4 shows five areas for privacy compliance management in which program managers and supervisors participate. As a measure of OPPC's effectiveness in cultivating an understanding of the various legal requirements in dealing with PII, all 20 managers of the programs we reviewed were able to articulate the privacy requirements for these areas. We address OPPC's efforts to ensure legal compliance in the following sections.

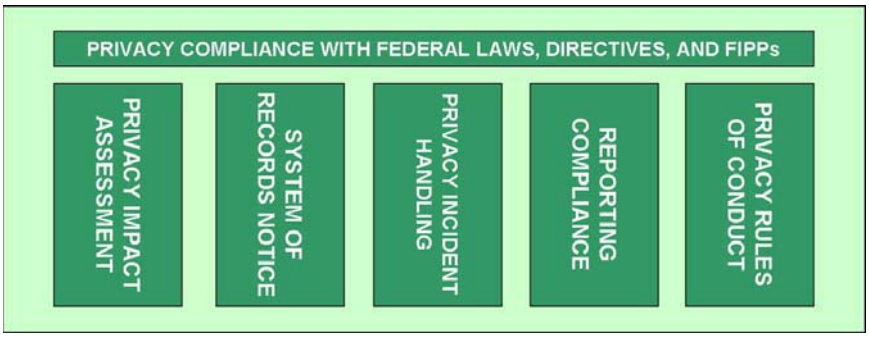


Figure 4. Privacy Compliance Management
Source: DHS Privacy Office

Privacy Impact Assessment

The *E-Government Act of 2002* requires agencies to conduct Privacy Impact Assessments (PIA) for information systems undergoing a certification and accreditation that collect, maintain, or disseminate PII.[3] TSA follows a two-part process for identifying and assessing information technology systems that collect or maintain PII.

During the first part of this process, managers complete a Privacy Threshold Analysis (PTA), which includes a description of the system, what PII, if any, is collected or used, and from whom. OPPC provides guidance and assistance to the managers regarding the development and preparation of the PTA, and approval of new or enhanced programs that may have privacy implications. OPPC forwards the completed PTA to the DHS Privacy Office to assist in identifying programs in DHS that use PII, evaluating changes to existing systems, determining the need for a PIA, and determining whether an existing System of Records Notice (SORN) will cover the new or enhanced program.[4]

[3] The PIA requirement of the *E-Government Act* has been extended by Office of Management and Budget Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003, to include technology that predates the *Act* if that technology has since undergone a significant change.

[4] The SORN is published in the *Federal Register*. A system of records is a group of any records about an individual under agency control from which information is retrieved by that individual's name, identifying number, symbol, or other identifying particular assigned to the individual. (5 U.S.C. § 552a(a)(5); TSA Management Directive 2100.2.)

During the second part of the process, managers complete a PIA to identify and assess privacy risks as precursors to determine what level of protections or controls are required to mitigate risks to PII. OPPC assists in the review of the proposed data elements to identify opportunities for PII minimization during the conduct of new and existing PIAs. The PIA includes the identification and analysis of the proposed collection methodology, analytical uses of data, privacy risks, and methods to mitigate risks. Almost 82% of surveyed managers indicated that they understand the PIA process and requirements.

OPPC reviews the completed PIAs, makes updates, and forwards documentation to the DHS Privacy Office. Once reviewed and approved by the DHS Privacy Office, unclassified PIAs are published in the *Federal Register* and on the DHS Privacy Office's internet website.

As required by the *E-Government Act*, TSA maintains an electronic inventory of 75 PII systems as of October 2008. To keep the PII inventory current, OPPC provides oversight of collection, use, dissemination, and maintenance of PII at TSA by scheduling annual discussions with program and system managers. (See appendix C for information regarding PIAs for the 10 PII programs that we reviewed.) OPPC formalized an annual review process as another analytical layer in TSA's PII review. This process requires written responses to standardized questions regarding the status of the PIA and SORN. Further, this process is intended to stimulate thinking about the FIPPs and privacy safeguards and identify key discussion items and areas for further review.

System of Records Notice

The *Privacy Act* mandates that agencies publish a SORN when they maintain PII in a system of records. The SORN explains how the public can exercise rights granted through the *Privacy Act* regarding the PII in that system of records. OPPC provides guidance and assistance to managers regarding the development and approval of systems of records. Almost 74% of surveyed managers and employees demonstrated knowledge of SORNs. (See appendix C for information regarding SORNs for the 10 PII programs that we reviewed.)

Further, OPPC reviews compliance with public notice requirements for systems of records or exemptions through the established process of reviewing PIAs and SORNs. The *Privacy Act* allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, it must issue a Notice of Proposed Rulemaking to explain why a particular exemption is claimed.

All of TSA's *Privacy Act* exemptions are published in the *Federal Register* and on the DHS Privacy Office internet website.

Privacy Incident Handling

DHS Action Memorandum, *Designation of Component Level Privacy Officers*, dated May 3, 2007, establishes that component-level privacy officers are the points of contact to handle privacy incident response.[5] TSA Management Directive 3700.4 establishes TSA's processes for reporting a privacy incident, detecting and minimizing the loss of privacy data, and notifying appropriate parties as required by the DHS Privacy Office's *Privacy Incident Handling Guidance*. Periodically, OPPC broadcasts messages with reminders that each employee controls the first step in preventing privacy violations.

OMB M-07-16 requires agencies to report all incidents involving PII to the United States Computer Emergency Readiness Team within an hour of the incident's discovery.[6] TSA had already established a core breach response group in January 2007 as recommended by OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, dated September 20, 2006. Further, as required by DHS Privacy Office's *Privacy Incident Handling Guidance*, OPPC reports suspected privacy incidents after reviewing them. TSA inspectors investigate the incidents, as necessary.

TSA complies with the OMB M-07-16 requirement for agencies to develop a notification policy and plan. As part of the notification procedures, OPPC follows an internal review process to evaluate the reasonable risk of harm associated with the incident to the affected individuals, and then issues notices to affected individuals, as appropriate.[7] As a best practice, the DHS Privacy Office adopted OPPC's template for providing notification of a privacy incident as the model for all DHS components.

[5] A privacy incident results from the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents involving PII that raise a reasonable risk of harm. (DHS Privacy Office, *Privacy Incident Handling Guidance*, § 2.4.11.)

[6] The United States Computer Emergency Readiness Team (US-CERT), a partnership between public and private sectors, also coordinates DHS incident response activities.

[7] Reasonable risk of harm refers to a likelihood that an individual on whom information is maintained may experience a substantial harm, embarrassment, inconvenience, or unfairness. (DHS Privacy Office, *Privacy Incident Handling Guidance*, § 2.4.13.)

Reporting Compliance

As required by OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act [(FISMA)] and Agency Privacy Management*, OPPC provides updated information—including incident response—to the DHS Privacy Office on its privacy management program as part of the overall reporting to OMB.[8] Congress and OMB review these results to evaluate agency-specific and government-wide security and privacy performance. In addition to its system security requirements, *FISMA* directs agencies to identify privacy risks intrinsic to each of its systems, develop ways to mitigate those risks, and report results of ongoing system assessments to OMB.

Privacy requirements and security controls are in different program areas within TSA. Therefore, OPPC consults with program officials, the chief information security officer, and information system security managers to review all circumstances that may reveal weaknesses in the privacy program for which remedial action, additional training, or development of internal guidance or policy may be appropriate.

Privacy Rules of Conduct

The *Privacy Act* requires privacy rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records.[9] OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, underscores the importance of privacy rules of conduct and the adoption of penalties for noncompliance. TSA disseminates its rules of privacy conduct and consequences to all employees and contractors involved with PII.

As required by the *Privacy Act*, TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information*, identifies responsibilities of TSA employees and requires their compliance with the *Privacy Act* and all DHS and TSA policies and regulations. This directive requires TSA supervisors to ensure that subordinates annually review their responsibilities in relation to the privacy policies and rules. TSA Management Directive 1100.73-5, *Employee Responsibilities and Conduct*, requires protection of information. Also, these rules of conduct are provided during the required online annual training. Some TSA programs require the acceptance of rules of privacy conduct prior to access to computers.

[8] OMB Memorandum 06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 17, 2006, provides reporting instructions for any physical or electronic incidents involving the loss of or unauthorized access to PII.

[9] *Privacy Act of 1974*, 5 U.S.C. § 552a (e)(9) (Establish Rules of Conduct.)

DHS Management Directive 0470.2, *Privacy Act Compliance*, requires that employees be advised of the possible consequences for violations of the *Privacy Act*. OPPC's goal is to ensure that the workforce understands the data it handles and the consequences for privacy policy violation. Almost 86% of surveyed employees indicated that they understand that there are penalties for violating the *Privacy Act*.

In response to a violation of TSA's rules of conduct, supervisors execute remedial, corrective, or preventative actions. When notified of privacy violations, OPPC follows up with supervisors to ensure that corrective action, such as retraining or issuing letters of counseling, is taken. When OPPC finds a systemic issue, it improves awareness through broadcast messages or training. Also, OPPC recommends disciplinary action. For example, when an individual broadcast PII to all persons in the office, although only one staff member needed to know such information, the violator was required to receive additional training on privacy information handling and was issued a letter of reprimand.

Established Processes for Notice, Complaints, and Redress for Individuals

Three privacy-related processes engage individual members of the public. As indicated in Figure 5, these processes address notice, complaints, and redress.

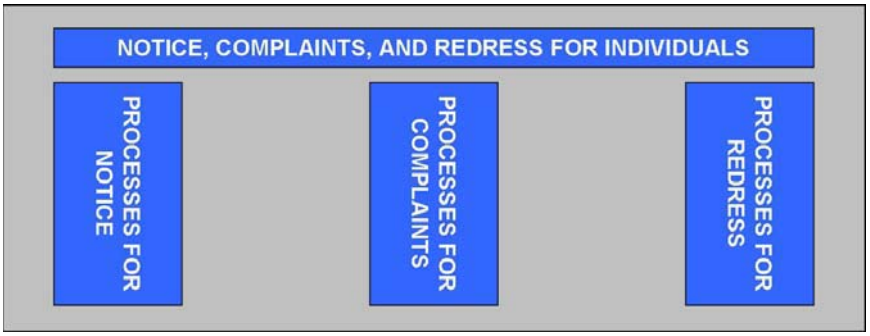


Figure 5. Notice, Complaints, and Redress for Individuals
Source: DHS Privacy Office

Processes for Notice for Individuals

The *Privacy Act* requires agencies to protect individuals by ensuring that personal information collected by federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions upon individual privacy.[10] TSA

[10] *Privacy Act of 1974*, 5 U.S.C. § 552a (e)(3) (*Privacy Act* Statement.)

provides a *Privacy Act* statement to all persons asked to provide personal information about themselves that will go into a system of records. OPPC reviews all TSA *Privacy Act* statements for compliance with the *Privacy Act*. DHS 4300A, *Sensitive Systems Handbook*, requires that DHS components present a security and privacy statement at every publicly accessible electronic entry point to agency websites. OPPC reviews the security and privacy statements before they are published on TSA's internet websites.

Processes for Complaints for Individuals

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* established additional privacy reporting requirements for DHS regarding reviews and complaints. For the purposes of reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with the DHS Privacy Office or TSA.[11] After addressing the privacy complaints or issues, OPPC forwards this information to the DHS Privacy Office in its quarterly reporting. Information on privacy complaints is available for public view on the DHS Privacy Office internet website.

TSA publishes information on how the public can issue a complaint or request redress (including correction) on its internet websites. As required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* § 803, TSA categorizes complaints as follows: (1) process and procedure issues, such as consent, appropriate notice at the time of collection, notices provided in the *Federal Register*, rules, or SORNs; (2) operational issues related to general privacy concerns and concerns not related to transparency or redress; (3) referrals to another federal agency or appropriate organization; or (4) redress issues related to appropriate access, correction, and redress, excluding the *Freedom of Information Act* and *Privacy Act* requests for access.[12] For the first three categories, OPPC is a point of contact for privacy complaints regarding process and procedures, operations, and referrals. Redress is handled separately, as described below.

Processes for Redress for Individuals

For redress and correction of their information, the Traveler Redress Inquiry Program (TRIP) is a single point of contact for individuals who have inquiries, seek resolution regarding difficulties they experienced

[11] DHS Privacy Office, *Privacy Policy Guidance Memorandum 2007-01*, allows complaints from U.S. Citizens and Lawful Permanent Residents, as well as visitors and aliens. (January 19, 2007, amended January 7, 2009.)
[12] *Freedom of Information Act* allows the right to request access to federal agency records, except those covered by any of nine exemptions. See 5 U.S.C. § 552(b).

during their travel screening at transportation hubs, or need correction of misidentifications during a credentialing process or traveler screening at airports.[13] Travel difficulties include being denied or delayed airline boarding; denied or delayed entry into or exit from the United States; and, continually referred for additional and secondary security screening. From July 31, 2007 through July 31, 2008, DHS TRIP received 31,206 redress requests; 2,100 of which were privacy related.

TSA also handles redress for transportation sector workers seeking credentials under TSA regulations. This population is estimated to exceed 7 million workers and covers populations, such as hazmat drivers and transportation and airport workers. TSA has established both appeals and waiver processes, and has received roughly 79,000 requests since inception.

Privacy Awareness and Training

DHS Management Directive 0470.2 requires that all employees be made aware of, and comply with, the *Privacy Act*. Toward that end, OPPC implements and monitors privacy awareness and training so that PII handlers understand risks, their own role in implementing privacy policies, and ways to mitigate those risks. As Figure 6 indicates, OPPC issues weekly newsletters, monthly privacy reminders, and posters to promote privacy awareness.

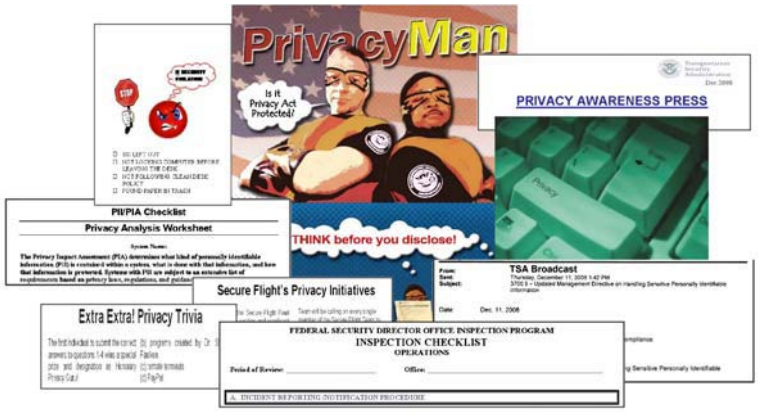


Figure 6. TSA Privacy Initiatives
Source: TSA documentation

[13] To address concerns about the high incidence of mistakes in the TSA watch lists, in 2004 Congress directed TSA to develop a prescreening process that would not produce a large number of false positives and would give misidentified airline passengers an effective way to correct the information in the database. In 2006, TSA's Office of Transportation Security Redress implemented the traveler redress website. The program evolved into the DHS Traveler Redress Inquiry Program (DHS TRIP) on February 21, 2007. DHS TRIP is managed by TSA and assisted by staff from various participating components.

Almost 83% of surveyed employees indicated positive effects of OPPC's privacy awareness, training, and guidance on their jobs. OPPC sends email reminders to alert employees to general privacy events and issues, posts privacy information on its intranet site for employee reference, and broadcasts messages on specific privacy guidance. TSA employees believe that the "Privacy Man" poster series is twice as effective as email or broadcast messages and recommend continuation of the poster campaign. One program—Secure Flight—has reminders in a section of its internal newsletter, "The Privacy Corner." Also, OPPC integrated privacy requirements into checklists used by airport and field inspectors.

OMB M-07-16 requires privacy training for new employees and annual privacy training for all employees. TSA uses standardized privacy materials from the DHS Privacy Office's "Culture of Privacy Awareness" training to meet these requirements. According to OPPC, nearly 100% of employees completed their 2008 privacy training. OPPC receives a monthly report from the TSA Online Learning Center listing employees who have not completed their required privacy training within a month of reaching their annual training threshold. OPPC contacts their supervisors to ensure that employees complete the training.

OPPC provides special training for program managers, information system security officers, and security officers. Almost 56% of surveyed employees also received advanced or specialized privacy training. Some managers or supervisors give their employees additional privacy training. Other TSA programs, such as Secure Flight, provide training based on roles and operation-specific rules of conduct. In addition to the required DHS Privacy Office's "Culture of Privacy Awareness" training, Secure Flight provides three additional levels of training for its personnel: "Privacy in Action" for Secure Flight managers and employees, reinforcement training, and advanced training.

Improvements to Privacy Effectiveness

TSA can improve its commitment to privacy effectiveness by having the Office of the Chief Information Officer (OCIO) implement automated privacy-specific tools for testing and monitoring. Further, TSA can implement innovative approaches to provide supplemental and job-specific privacy awareness or training activities.

Automated Privacy-Specific Tools for Testing and Monitoring

The *Privacy Act* requires federal agencies to establish appropriate administrative, technical, and physical safeguards to protect PII against

any anticipated threats or hazards to its security or integrity. Further, the FIPPs require that TSA protect PII through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. TSA Management Directive 2100.2 establishes OPPC's oversight responsibility for PII and for privacy policy implementation. However, the OCIO is responsible for securing data, including PII, for all TSA systems and services. According to DHS Management Directive 0007.1, *Information Technology Integration and Management*, OCIO directs timely delivery of mission information technology (IT) services in direct support of a component's mission, goals, objectives, and programs, and provides management and administration of all component IT resources and assets to meet mission, department, and enterprise program goals.

Because automated privacy tools for testing and monitoring are not provided by the OCIO, OPPC has been checking periodically for PII data leakage by performing manual searches on TSA's file servers that should not contain PII or should be password-protected to limit access. Data leakage is the exposure or transmission of PII that permits unauthorized access or disclosure. PII data was found that should not have been accessible through the periodic checks. Further, according to TSA, data spills, unprotected emails of personnel information, and lost folders containing PII have occurred.

Although OPPC implements privacy policies and interacts with personnel, OCIO cannot electronically monitor privacy behavior continuously and measure the strength of PII protections. TSA has not purchased tools and technologies to automate privacy protections because further research and collaboration by OPPC and OCIO is necessary to identify requirements and appropriate approaches within the TSA computing environment. Without privacy-focused measurements and testing, TSA cannot compare the levels of PII protections across different systems containing PII and improve overall privacy data protection and monitoring.

More Effective Privacy Awareness and Training Are Needed

To promote and improve daily awareness of employees' privacy responsibilities, OMB M-07-16 recommends that agencies augment training using creative methods, job-specific communications, and advanced training commensurate with the employees' responsibilities.[14] According to DHS Action Memorandum, dated May 3, 2007, OPPC is responsible for implementing and monitoring training for TSA employees

[14] Office of Management and Budget Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

in coordination with the DHS Privacy Office. TSA provides required computer-based annual privacy training for employees and offers specialized privacy training to groups such as program and security managers. TSA augments required privacy training through some awareness activities, such as the "Privacy Man" poster series. However, OPPC, based on perceived organizational needs, has implemented a limited scaled privacy awareness campaign.[15] Secure Flight works with OPPC to improve program-level understanding of how to integrate privacy requirements into its operations.

However, out of 875 survey responses that provided written comments, 469 employees wanted improvements in privacy awareness and training. These improvements, illustrated in Figure 7, address five categories: vary delivery method of privacy training (26%); provide more job-specific privacy training (17%); develop more privacy awareness activities (26%); increase frequency of privacy training (26%); and, improve communication of privacy requirements (5%).

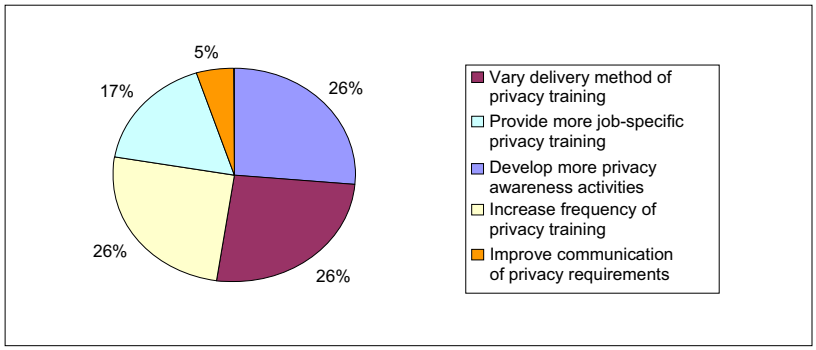


Figure 7. Improvements for Privacy Awareness and Training
Source: OIG analysis

TSA relies on computer-based privacy training from the DHS Privacy Office to meet the *Privacy Act* annual training requirement. The primary delivery methods for TSA's privacy communications and policies are also electronic. However, the computerized delivery method does not meet the unique needs of the TSA workforce. TSA has a large workforce spread over a wide geographical area, and an estimated 80% of employees have limited access to computers. The computerized delivery may limit the overall effectiveness of the training.

[15] A comprehensive privacy awareness campaign could include privacy awareness week; privacy cleanup day; training classes tailored for specific privacy needs; privacy events; email advisories; newsletters; periodicals, intranet privacy daily news; posters; do and don't lists; warning banners/messages; and reward programs that include privacy letters of appreciation.

Extending beyond the control of OPPC, organizational commitment, collaboration, and resources are necessary to implement a large-scale, innovative privacy awareness and training program. According to 74% of surveyed employees, TSA needs more frequent and effective privacy awareness, job-specific training, and privacy communications. TSA employees need to be continually reminded of the importance in protecting PII and preventing privacy incidents.

Recommendations

We recommend that the TSA Administrator:

Recommendation #1: Direct the Office of the Chief Information Officer to implement automated privacy-specific tools for testing and monitoring.

Recommendation #2: Implement approaches to provide supplemental and job-specific privacy awareness or training activities for the TSA workforce.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the TSA Acting Administrator. We have included a copy of the comments in appendix B.

The Acting Administrator concurred with our findings and recommendations. We consider our recommendations resolved, but open pending our review of actions taken by TSA.

Appendix A
Purpose, Scope, and Methodology

Our objective was to determine whether TSA's plans and activities instill and promote a privacy culture and comply with federal privacy laws and regulations. As background for this audit, we researched and reviewed federal guidance and laws related to TSA's responsibilities for privacy protections. We reviewed testimonies, TSA documentation, and reports related to TSA's privacy, information technology security, and program management.

We interviewed officials from the DHS Office of the Chief Information Officer and the DHS Privacy Office. With the latter, we discussed its implementation of the DHS Privacy Framework and duties for component privacy officers. In addition to interviewing TSA's Office of Privacy Policy and Compliance and chief information security officer, we interviewed more than 65 program managers and information system security professionals at TSA headquarters and field sites regarding privacy activities. We surveyed 2,285 TSA employees on their knowledge of the *Privacy Act*, PII handling, privacy incident response, and privacy stewardship. Of this survey group, 875 employees offered written comments on the status, issues, suggestions, or challenges in TSA privacy stewardship. (See appendix G.)

We selected a sample of 16 systems (that support 10 programs) from a total of 75 systems that handle personally identifiable information. We reviewed technical information, system security documentation, architectures, financial justifications, privacy impact assessments, system of records notices, application of the Fair Information Practice Principles, and TSA and program-level application of privacy policies.

Our analysis is based on direct observation, review of applicable documentation, and interviews. We conducted this performance audit between August 2008 and May 2009 in accordance with generally accepted government auditing standards. The 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits at (202) 254-4041, and Marj Leaming, Director, System Privacy Division at (202) 254-4172. Major OIG contributors to the audit are identified in appendix I.

Appendix B
Management Comments to the Draft Report

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

Transportation Security Administration

AUG 19 2009

INFORMATION

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for
Information Technology

FROM: Keith Kauffman for,
Gale D. Rossides
Acting Administrator

SUBJECT: Transportation Security Administration's (TSA) Response to the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Report, *Transportation Security Administration Privacy Stewardship,* July 2009

Purpose

This memorandum constitutes TSA's response to Draft Report, *Transportation Security Administration Privacy Stewardship*, July 2009. TSA expresses its thanks to the OIG for acknowledging TSA's progress in implementing a framework that promotes a privacy culture and complies with Federal privacy laws and regulations. Overall, TSA concurs with the draft report's recommendations on how to continue to improve its privacy program.

Background

From August 2008 through May 2009, OIG conducted an audit to determine whether TSA's plans and activities instill and promote a privacy culture and comply with Federal privacy laws and regulations. As background for the audit, the OIG researched and reviewed Federal guidance and laws related to TSA responsibilities for privacy protections. The OIG interviewed officials from the DHS Office of the Chief Information Officer, the DHS Privacy Office, TSA's Office of Privacy Policy and Compliance, and TSA's Chief Information Security Officer. OIG also interviewed more than 65 program managers and information system security professionals at TSA headquarters and field sites regarding privacy activities. The OIG conducted a survey of 2,285 TSA employees on their knowledge of the Privacy Act, Personally Identifiable Information (PII) handling, privacy incident responses and privacy stewardship. Of the employees surveyed, 875 employees offered written comments on the status, issues, suggestions, or challenges in TSA privacy stewardship. The OIG reviewed testimonies, TSA documentation, and reports related to TSA privacy, information technology security, and program management.

Discussion

TSA's Office of Privacy Policy and Compliance (OPPC) continues to strengthen its mission to respect and protect the privacy of individuals affected by our activities, as well as that of our employees. There are privacy elements to every aspect of the collection, maintenance, disclosure, and destruction of information about individuals. TSA will continue to ensure that its customers and employees know they are the most important component in implementing an effective privacy program at TSA and protecting individuals from harms that may arise when privacy is not adequately considered.

Attachment

Appendix B
Management Comments to the Draft Report

Transportation Security Administration (TSA) Response to Office of the Inspector General (OIG) Draft Report, *Transportation Security Administration Privacy Stewardship*, July 2009

Recommendation No. 1: Direct the Office of the Chief Information Officer to implement automated privacy-specific tools for testing and monitoring.

TSA Concurs. TSA has a robust testing team that is skilled in the use of a variety of tools to detect vulnerabilities that may expose PII, including web, application, and database vulnerabilities. Vulnerabilities found during internal assessments, security testing and evaluation, and continuous monitoring are tracked and remediated in accordance with risk management best practices, National Institute of Standards and Technology (NIST) Special Publication 800-30, DHS 4300A, and TSA 1400.3. TSA has investigated real-time, privacy-specific monitoring tools and expects to continue efforts to identify products that perform appropriately. Funding for future implementation of such tools has been requested.

Recommendation No. 2: Implement approaches to provide supplemental and job specific privacy awareness or training activities for the TSA workforce.

TSA Concurs. TSA has undertaken a wide variety of training and awareness efforts, including the highly popular "Privacy Man" series of posters, e-mail broadcast messages, use of the "remarks" field within the bi-weekly Leave and Earnings Statement, individualized training to managers, speeches at Townhall meetings, distribution of Privacy Awareness Press, and mandatory online training. TSA also maintains an informative intranet website addressing privacy matters for its employees. More than half of the employees surveyed by the OIG for this report stated they had received specialized or advanced privacy training. Nevertheless, TSA recognizes that in any large organization constant training and outreach are critical components to an effective privacy program. TSA recently distributed "Privacy Please" door hangers with office contact information and "do's and don'ts," and broadcast an e-mail message on the mechanics of restricting access to shared drives.

Appendix C
Programs Reviewed During This Audit

Program Name & Mission	Privacy Impact Assessment	System of Records Notice
THREAT ASSESSMENT & CREDENTIALING		
Alien Flight Student Program (AFSP) Conduct the security threat assessments of alien flight students	Transportation Security Administration's Alien Flight Student Program (Amended), December 22, 2006	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
Crew Vetting Program (CVP) Conduct security threat assessments of airline crew members	Crew Vetting Program, July 28, 2004	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
Hazardous Material Fingerprints (HAZPRINT) Perform threat assessments of hazardous material drivers	TSA Hazardous Materials Endorsement, Amendment, September 16, 2005	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
Secure Flight (SF) Match identifying information of aviation travelers against the terrorist watch list	Transportation Security Administration's Secure Flight Program, October 21, 2008	Secure Flight Records DHS/TSA 019, November 9, 2007, 72 FR 63711
Transportation Worker Identification Credential (TWIC) Provide a biometric credential to confirm national transportation system worker identity	Transportation Security Administration's Transportation Worker Identification Credential Program Final Rule, October 5, 2007	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
Indirect Air Carrier Management System (IACMS) Screen cargo transported aboard passenger aircraft	Air Cargo Security Requirements, November 12, 2008	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
Known Shipper Management System (KSMS) Screen cargo transported aboard passenger aircraft	Air Cargo Security Requirements, November 12, 2008	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
LAW ENFORCEMENT		
Federal Flight Deck Officer Dashboard (FFDO) Deputize volunteer aircraft personnel to defend the flight deck against acts of criminal violence or air piracy	Transportation Security Administration's Federal Flight Deck Officer Program, January 10, 2008	Federal Flight Deck Officer Record System DHS/TSA 013, August 18, 2003, 68 FR 49496
Tactical Information Sharing System (TISS) Share transportation security intelligence with federal, state, and local law enforcement	Transportation Security Administration's Tactical Information Sharing System, June 1, 2008	Transportation Security Threat Assessment System DHS/TSA 002, November 8, 2005, 70 FR 33383
REDRESS		
Traveler Redress Inquiry Program (TRIP) Provide a one-stop mechanism for individual redress	The Department of Homeland Security Traveler Redress Inquiry Program, January 18, 2007	Department of Homeland Security Redress and Response Records System DHS/ALL-005, January 18, 2007, 72 FR 2294

Source: The DHS Privacy Office at http://www.dhs.gov/xabout/structure/editorial_0338.shtm. This page, which was last reviewed/modified on March 12, 2009, has the TSA Privacy Impact Assessments and System of Records Notices. The program missions are found in the respective Privacy Impact Assessments.

Appendix D
Cross Reference of DHS Privacy Framework With Component Privacy Officer Duties

DHS PRIVACY FRAMEWORK – FUNCTIONAL AREAS
ORGANIZATIONAL COMMITMENT TO PRIVACY Establish organizational oversight and implement privacy activities. - Responsible for effectively communicating, in coordination with the DHS Privacy Office, privacy initiatives associated with TSA with a variety of internal and external constituents, including the media, industry stakeholders, various offices within DHS and other federal agencies. - Serve as the Chief Privacy Officer's main point of contact at TSA to implement the policies and directives of the DHS Privacy Office in carrying out Section 222 of the *Homeland Security Act of 2002*, as amended.
POLICIES FOR PROPER HANDLING OF PII Define and promote privacy policies and procedures. - Identify privacy issues related to TSA and apply appropriate privacy policies in accordance with federal privacy laws, and DHS and TSA policies developed to ensure that TSA protects the privacy of individuals affected by its activities.
PRIVACY COMPLIANCE MANAGEMENT Implement tools and processes for privacy compliance (including reporting requirements, privacy impact assessments, systems of records notice, privacy incident handling, and privacy rules of conduct). - Assist in draft and review PTAs, PIAs, and SORNs, as well as any associated privacy documentation, as dictated by DHS Privacy Office policy and required by law, including the *Privacy Act of 1974*, the *E-Government Act of 2002*, and the *Homeland Security Act of 2002*. - Provide oversight on the collection, use, dissemination, and maintenance of PII at TSA. - Serve as TSA's privacy point of contact to handle privacy incident responses as defined in the DHS Privacy Office's *Privacy Incident Handling Guide* for all TSA disclosures involving PII. - Provide to the DHS Privacy Office information related to privacy, in coordination with the TSA information system security manager necessary for the quarterly and annual *FISMA* reporting - Monitor TSA's compliance with all applicable federal privacy laws and regulations, implement corrective, remedial, and preventive actions and notify the DHS Privacy Office of privacy issues or any non-compliance, whenever necessary.
NOTICE, COMPLAINTS, AND REDRESS FOR INDIVIDUALS Establish processes for notices, complaints, and redress for individuals. - Provide oversight on the collection, use, dissemination, and maintenance of PII at TSA.
PRIVACY AWARENESS AND TRAINING Support privacy requirements through privacy awareness and training. - Implement and monitor training for TSA employees in coordination with the DHS Privacy Office.

Source for Component Privacy Officer Duties: DHS Privacy Office Action Memorandum, *Designation of Component Level Privacy Officers*, May 3, 2007. (OIG applied to TSA.)

Appendix E
Cross Reference of DHS Privacy Framework With Criteria Applied to TSA Privacy Stewardship

As part of its privacy framework, the DHS Privacy Office identified five functional areas necessary for component privacy officers to promote a culture of privacy. As part of the TSA Privacy Stewardship audit, OIG applied criteria to TSA's functional areas as described below.

DHS PRIVACY FRAMEWORK – FUNCTIONAL AREAS
ORGANIZATIONAL COMMITMENT TO PRIVACY Establish organizational oversight and implement privacy activities. - TSA Management Directive 2100.2, *Privacy and Information Collection Policy* (establish OPPC oversight for PII and privacy implementation) - TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information* (establish OPPC responsibility for privacy management in compliance with federal privacy laws, directives, and the FIPPs) - DHS Privacy Office Action Memorandum, *Designation of Component Level Privacy Officers*, May 3, 2007 (organizational oversight of PII) - DHS Management Directive 0470.2, *Privacy Act Compliance* (privacy compliance and awareness) - OMB M-05-08, *Designation of Senior Agency Officials for Privacy* - OMB Circular A-130, *Management of Federal Information Resources* (privacy management) - *Privacy Act of 1974* (establish safeguards to protect PII) - Fair Information Practice Principles (accountability, auditing, security)
POLICIES FOR PROPER HANDLING OF PII Define and promote privacy policies and procedures. - TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information* (establish policies and procedures for privacy compliance) - DHS 4300A, *Sensitive Systems Handbook* (privacy statement at publicly accessible entry) - DHS Privacy Office Action Memorandum, *Designation of Component Level Privacy Officers*, May 3, 2007 (implement privacy laws, policies, and directives) - OMB M-06-15, *Safeguarding Personally Identifiable Information* (establish safeguards to protect PII) - OMB M-06-19, *Reporting Incidents Involved Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (privacy rules of conduct) - *Privacy Act of 1974* (establish safeguards to protect PII) - Fair Information Practice Principles (PII purpose, use limitation, security)
PRIVACY COMPLIANCE MANAGEMENT Implement tools and processes for privacy compliance (including reporting requirements, privacy impact assessment, system of records notice, privacy incident handling, and privacy rules of conduct). - TSA Management Directive 2100.2, *Privacy and Information Collection Policy* (privacy impact assessment, system of records notice) - TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information* (handling sensitive PII, privacy incident handling, employee responsibility) - DHS Privacy Office, *Privacy Incident Handling Guidance* - DHS Management Directive 0470.2, *Privacy Act Compliance* (privacy compliance and awareness) - DHS Privacy Office Action Memorandum, *Designation of Component Level Privacy Officers*, May 3, 2007 (privacy incident response) - OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act* (post website privacy notices, privacy impact assessments) - OMB M-06-15, *Safeguarding Personally Identifiable Information* (privacy rules of conduct) - OMB M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (reporting compliance) - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (privacy rules of conduct) - OMB Circular A-130, *Management of Federal Information Resources* (privacy reporting) - *Privacy Act of 1974* (privacy rules of conduct, system of records notice, establish safeguards to protect PII) - *E-Government Act of 2002* (post website privacy notices, privacy impact assessments, electronic inventory of PII)

Appendix E
Cross Reference of DHS Privacy Framework With Criteria Applied to TSA Privacy Stewardship (continued)

- *Federal Information Security Management Act of 2002* (agency-wide information security program) - Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (privacy reporting requirements) - Fair Information Practice Principles (accountability, auditing, security)
NOTICE, COMPLAINTS, AND REDRESS FOR INDIVIDUALS Establish processes for notices, complaints, and redress for individuals. - DHS 4300A, *Sensitive Systems Handbook* (privacy statement at publicly accessible entry) - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (notice) - OMB Circular A-130, *Management of Federal Information Resources* (complaints, redress) - Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (reporting complaints, redress) - *Privacy Act of 1974* (notices, complaints, redress) - Fair Information Practice Principles (notices, complaints, redress)
PRIVACY AWARENESS AND TRAINING Support privacy requirements through privacy awareness and training. - TSA Management Directive 3700.4, *Handling Sensitive Personally Identifiable Information* (employee compliance with *Privacy Act*, DHS, and TSA privacy policies) - DHS Privacy Office Action Memorandum, *Designation of Component Level Privacy Officers,* May 3, 2007 (monitor privacy training) - DHS Management Directive 0470.2, *Privacy Act Compliance* (privacy compliance and awareness) - OMB M-06-15, *Safeguarding Personally Identifiable Information* (privacy training) - OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (privacy training and awareness) - *Privacy Act of 1974* (privacy rules of conduct) - Fair Information Practice Principles (accountability, training)

Source: DHS Privacy Office (OIG added criteria as applied to TSA's privacy efforts.)

Appendix F
Fair Information Practice Principles

The DHS Privacy Office, Privacy Policy Guidance Memorandum Number: 2008-01, December 29, 2008, adopted the Fair Information Practice Principles as its privacy policy framework for application by DHS programs and activities. The following are the eight specific principles that guide privacy policy.

THE FAIR INFORMATION PRACTICE PRINCIPLES
Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS use of PII.
Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
Data Minimization: DHS should collect only PII that is directly relevant and necessary to accomplish the specified purpose(s) and retain PII only for as long as is necessary to fulfill the specified purpose(s).
Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the department should be for a purpose compatible with the purpose for which the PII was collected.
Data Quality and Integrity: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

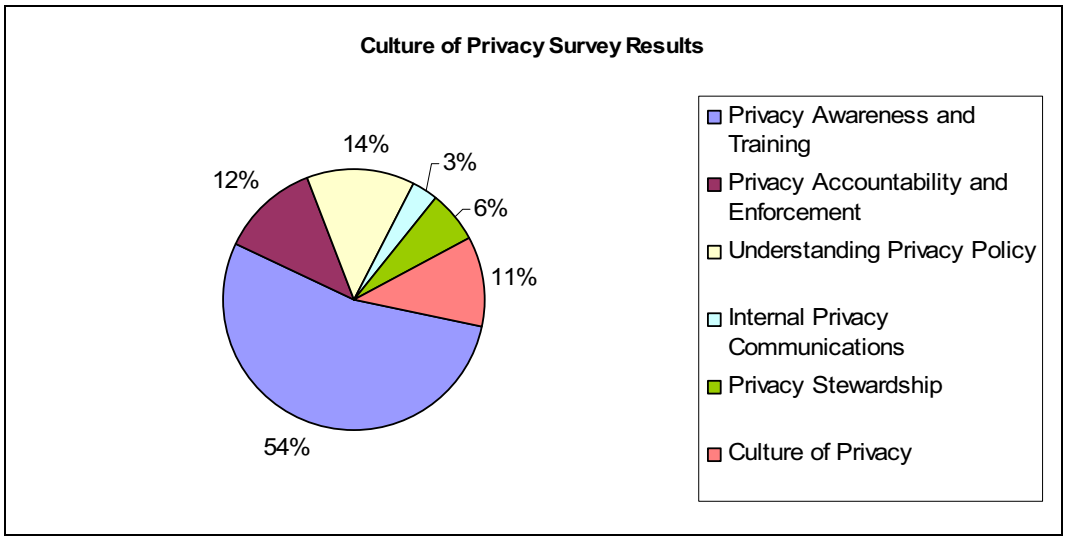
Appendix G
TSA Culture of Privacy Survey

From November through December 2008, we surveyed TSA personnel to determine their level of privacy awareness and knowledge and to obtain recommendations for improving privacy management. We developed the privacy questionnaire with OPPC's involvement to ensure compatibility with TSA's existing privacy culture. TSA personnel were emailed a link to a secure site to complete an online privacy questionnaire. All 2,285 responses were confidential, and results were accessible only by the OIG. The portion of the survey that addressed knowledge of privacy was derived from, but not limited to, the criteria in appendix E.

DEMOGRAPHICS OF PARTICIPANTS OF TSA CULTURE SURVEY
Level of Job Responsibility - Entry-level employees (27.3%) - Mid to high-level (non-manager) employees (40.7%) - Supervisors/managers (32.0%)
Location - Headquarters (8.1%) - Field offices (70.1%) - Operation centers (4.2%) - Other (17.6%)
Length of Service - Less than 3 months (2.8%) - 3–12 months (9.3%) - 1–3 years (13.6%) - More than 3 years (74.3%)

Source: OIG Culture of Privacy Survey

TSA personnel provided 875 additional written comments regarding privacy awareness and training, privacy accountability and enforcement, understanding privacy policy, internal privacy communications, privacy stewardship, and culture of privacy. The following figure summarizes these results.



Source: OIG Culture of Privacy Survey

Appendix H
Laws, Regulations, Directives, and Guidance Related to TSA Privacy Stewardship

LEGISLATION

Privacy Act of 1974, 5 U.S.C. § 552a. (1974). http://www.opm.gov/feddata/USC552a.txt

E-Government Act of 2002, Public Law 107-347, 44 U.S.C. Ch 36. (2002). http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq. (2002). http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266, 360. (2007). http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf

OMB MEMORANDA

OMB M-06-20: *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. (July 17, 2006). http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. (May 22, 2007). http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

DIRECTIVES AND GUIDANCE

DHS Management Directive Number 0470.2: *Privacy Act Compliance*. (October 6, 2005). (No external link.)

DHS 4300A: *Sensitive Systems Handbook*. (July 2009). (No external link.)

DHS Privacy Office: *Privacy Incident Handling Guidance*. (September 10, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

DHS Privacy Office Action Memorandum: *Designation of Component Level Privacy Officers*. (May 3, 2007). (No external link.)

DHS Privacy Policy Guidance Memorandum Number 2008-01: *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*. (December 29, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

TSA Management Directive Number 3700.4: *Handling Sensitive Personally Identifiable Information*. (December 9, 2008). (No external link.)

TSA Management Directive Number 2100.2: *Privacy and Information Collection Policy*. (July 25, 2005). (No external link.)

System Privacy Division

Marj Leaming, Director
Eun Suk Lee, Lead Privacy Auditor
Philip Greene, System Privacy Auditor
Cory Missimore, Privacy Specialist
Zach Miller, Management and Program Assistant

Shannon Frenyea, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
Acting 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
Administrator for Transportation Security Administration
Transportation Security Administration Audit Liaison
Chief Privacy Officer
Officer for Civil Rights and Civil Liberties

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, please call the Office of Inspector General (OIG) at (202) 254-4100, 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;

• Email 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.