



Department of Homeland Security Office of Inspector General

U.S. Citizenship and Immigration Services Privacy Stewardship





**Homeland
Security**

MAY 24 2011

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 U.S. Citizenship and Immigration Services' plans and activities to instill a privacy culture that protects sensitive personally identifiable information and ensure 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.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank Deffer

Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	4
USCIS Has Made Progress With Privacy Stewardship	4
Privacy Risks to A-Files Need Mitigation	7
Recommendations.....	10
Management Comments and OIG Analysis	11
Technical Risks to PII Need to Be Addressed.....	12
Recommendation	13
Management Comments and OIG Analysis	14
Physical Security Standards Need Consistent Enforcement to Protect PII.....	15
Recommendation	16
Management Comments and OIG Analysis	16
Privacy Training and Awareness Need Improvement to Increase Effectiveness	18
Recommendations.....	21
Management Comments and OIG Analysis	21

Figures

Figure 1:	Purposes for Personally Identifiable Information in a Typical Day at USCIS	2
Figure 2:	Pillars of Privacy Stewardship	3
Figure 3:	Stages of Processing Alien Registration Files Containing Personally Identifiable Information	8
Figure 4:	Examples of Alien Registration Files	9
Figure 5:	Service Center Telework Participation/Monthly Missing Alien Registration Files Rates in 2009	9
Figure 6:	Examples of Controls for Physical Access	15
Figure 7:	<i>Records Are People, People's Lives</i>	20

Appendices

Appendix A:	Purpose, Scope, and Methodology.....	22
Appendix B:	Management Comments to the Draft Report	24
Appendix C:	Legislation, Memoranda, Directives, and Guidance Pertinent to the USCIS Privacy Stewardship Audit.....	31
Appendix D:	Component Level Privacy Office Designation and Duties.....	33
Appendix E:	USCIS Systems: Privacy Impact Assessments and System of Records Notices	34

Appendix F: OIG Privacy Culture Survey	38
Appendix G: Major Contributors to this Report.....	40
Appendix H: Report Distribution	41

Abbreviations

A-File	Alien Registration File
DHS	Department of Homeland Security
FISMA	<i>Federal Information Security Management Act of 2002</i>
MD	Management Directive
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSI	Office of Security and Integrity
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
SORN	System of Records Notice
USCIS	U.S. Citizenship and Immigration Services

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We performed an audit of U.S. Citizenship and Immigration Services' privacy stewardship. Our audit objectives were to determine whether the plans and activities of U.S. Citizenship and Immigration Services instill a culture of privacy and whether they comply with federal privacy laws and regulations.

U.S. Citizenship and Immigration Services demonstrated an organizational commitment to privacy stewardship by appointing a privacy officer and establishing its Office of Privacy. The Office of Privacy monitors compliance with federal privacy laws and regulations and provides guidance to managers and employees on meeting requirements for notice, incident reporting, and privacy impact assessments. In addition, the Office of Privacy conducts initial and annual privacy training and addresses inquiries and complaints by individuals.

While U.S. Citizenship and Immigration Services has made progress in implementing a privacy program that complies with privacy laws, opportunities still exist to improve its privacy culture. Specifically, management can improve the protection of Alien Registration Files by conducting a privacy risk analysis on telework and adjudication activities at service centers and field offices. Also, technical vulnerabilities regarding removable data devices, email, and system auditing and monitoring need to be addressed. Further, physical security standards need to be implemented consistently in all U.S. Citizenship and Immigration Services facilities. Management must ensure that employees and contractors are receiving mandatory privacy training, along with appropriate job-specific, advanced, or specialized application of privacy training and awareness. We are making six recommendations to the Deputy Director of U.S. Citizenship and Immigration Services to strengthen its culture of privacy.

Background

U.S. Citizenship and Immigration Services (USCIS) is responsible for granting immigration and citizenship benefits, promoting an understanding of citizenship, and ensuring the integrity of our immigration system. Interacting with the public in more than 250 offices around the world, almost 18,000 USCIS employees collect, use, and disseminate personally identifiable information (PII). PII refers to 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, whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the United States.

USCIS' main customers are immigrant and nonimmigrant applicants or petitioners for benefits or services. Figure 1 lists purposes for which USCIS collects PII from the public in a typical day.

Figure 1. Purposes for Personally Identifiable Information in a Typical Day at USCIS

PURPOSES FOR PERSONALLY IDENTIFIABLE INFORMATION IN A TYPICAL DAY AT USCIS
<ul style="list-style-type: none">• Conduct 135,000 national security background checks• Complete 30,000 applications for various immigration benefits• Fingerprint and photograph 11,000 applicants• Process 3,700 applications to sponsor relatives and fiancées• Ensure employment eligibility of more than 80,000 new hires

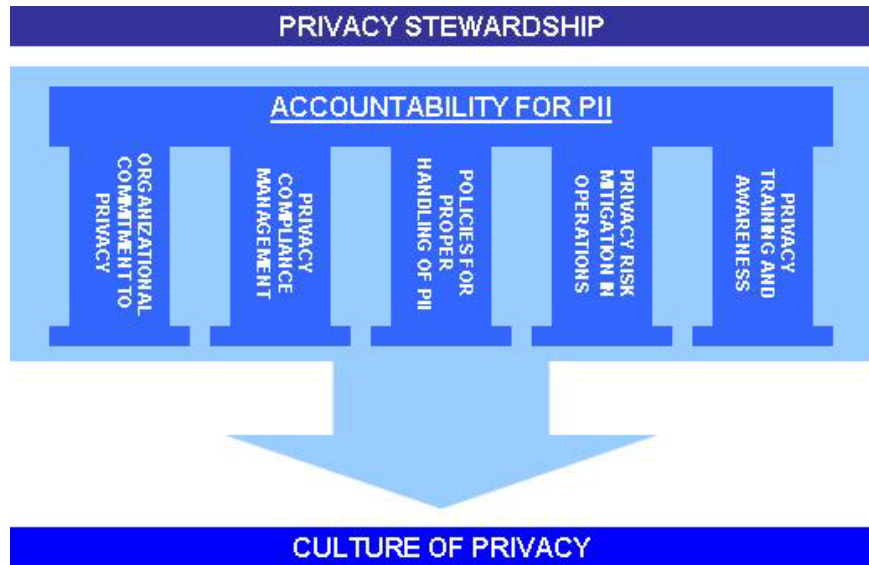
Source: USCIS.

The *Privacy Act of 1974*, as amended, imposes requirements on agencies whenever they collect, use, or disseminate PII in a system of records. The Privacy Act grants access and amendment rights to U.S. citizens and legal permanent residents.¹

As illustrated in Figure 2, our review of effective privacy stewardship includes assessing 1) organizational commitment to privacy, 2) privacy compliance management, 3) policies for proper handling of PII, 4) privacy risk mitigation in operations, and 5) privacy training and awareness.

¹ DHS Privacy Office, *Policy Guidance Memorandum Number 2007-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, extends privacy protection to non-U.S. persons to have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act. However, this policy does not extend or create a right of judicial review for non-U.S. persons.

Figure 2. Pillars of Privacy Stewardship



Source: Office of Inspector General (OIG) analysis.

A component's culture of privacy results from how well its executive leadership, managers, and employees understand, implement, and enforce its privacy commitment. Privacy stewardship, or the promotion of an effective culture of privacy, leads to embedded shared attitudes, values, goals, and practices for complying with the requirements for proper handling of PII. A component privacy officer can help enhance the privacy culture by identifying privacy issues and working within the component to address them.

Results of Audit

USCIS Has Made Progress With Privacy Stewardship

USCIS has made progress in promoting a culture of privacy across the agency. Specifically, it established an Office of Privacy in November 2007 and designated a privacy officer who is responsible for performing certain duties, as required by the DHS Memorandum *Designation of Component Privacy Officers*, dated June 5, 2009. See Appendix D for a description of each specific duty.

USCIS Office of Privacy

The Privacy Officer reports to the USCIS Director's Chief of Staff and works collaboratively with the DHS Privacy Office by serving as its point of contact and participating in its working groups. The Office of Privacy consists of four staff members who perform the following duties to improve the culture of privacy in USCIS:

- Advises USCIS leadership, management, and staff on matters with privacy impact.
- Develops and issues DHS/USCIS privacy policy guidance.
- Provides advice and technical assistance in the development of privacy compliance documentation.
- Manages PII incident response.
- Develops and administers privacy awareness training.

Initial and Annual Privacy Training

To comply with Office of Management and Budget (OMB) M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, USCIS provides initial privacy training for new employees and annual refresher privacy training for current employees. Throughout 2009 and 2010, the Office of Privacy conducted 23 privacy training sessions at field locations throughout the country. Also, the Office of Privacy collaborated with the Office of Human Capital and Training to monitor privacy training completion by the workforce. For example, in FY 2009, USCIS reported that more than 95% of its employees completed annual refresher privacy training.

Privacy Impact Assessments

The *E-Government Act of 2002* requires agencies to conduct Privacy Impact Assessments (PIAs) for information systems that

collect, maintain, or disseminate PII. A PIA helps the public understand what PII is being collected, why it is being collected, and how it will be used, shared, accessed, and stored. As part of preparing a PIA, the Office of Privacy helps managers to analyze their use of proposed PII collections, as well as privacy risks and their mitigation throughout the life cycle of a program or system.

USCIS has 34 PIAs that are approved by the DHS Privacy Office and are available on its public website. See Appendix E for a list and description of these PIAs.

Systems of Records Notices

The Privacy Act requires federal agencies to issue Systems of Records Notices (SORNs) for every system of records under their control that collects PII and from which information is retrieved by an identifier. 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. The Office of Privacy assists managers in determining whether they have a system of records.

The SORNs are published in the *Federal Register* to explain to the public the purpose for which PII is collected for a particular system of records, from whom the information is collected, and what type of PII is collected, how that information is shared externally, and how the public can exercise rights granted through the Privacy Act regarding the PII in a system of records. USCIS has 12 SORNs and three exemptions that are approved by the DHS Privacy Office and available on its public website.²

Reporting Privacy Status and Incident Handling

The *Federal Information Security Management Act of 2002* (FISMA) directs agencies to identify privacy risks intrinsic to their systems, develop ways to mitigate those risks, and report results of ongoing system assessments to OMB. The Office of Privacy updates the status of privacy information required by FISMA.

The DHS Privacy Office *Privacy Incident Handling Guidance* establishes responsibilities for the Office of Privacy to perform.

² 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.

The Office of Privacy reviews suspected privacy incidents, determines whether the incidents relate to privacy, and if so, provides an analysis of ways to minimize the loss of privacy data. The office evaluates the reasonable risk of harm associated with the incident to the affected individuals, and issues notices to the affected individuals, if appropriate.

Processes for Privacy Notice and Complaints for Individuals

The Privacy Act requires agencies to provide notice to individuals prior to the collection of their PII, absent an exemption under the Privacy Act. The Office of Privacy assists managers with the drafting of notices on forms or websites.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* defines complaints as written allegations of harm or violation of privacy compliance requirements that may include requests for access, correction, and redress from individuals. Complaints may be filed with the DHS Privacy Office or USCIS. USCIS has processes to receive privacy complaints or requests for access, correction, and redress from individuals. Individuals may file complaints through the Ombudsman Office or specific program offices, such as the Verification Division. The Office of Privacy reviews all pertinent privacy issues.

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* also establishes additional privacy reporting requirements for complaints regarding DHS. In July 2010, the Office of Privacy implemented a system to track and resolve privacy complaints and requests for access, correction, and redress. The DHS Privacy Office public website contains information on USCIS and other component privacy complaints.

Privacy Risks to A-Files Need Mitigation

USCIS has not identified ways to mitigate privacy risks when transporting PII, primarily contained in Alien Registration Files (A-Files). First, USCIS does not have PIAs that identify vulnerabilities and establish ways to protect A-Files when they are physically moved from one operation to another or transported among USCIS facilities. Second, USCIS has not provided rules of conduct, as required by the Privacy Act, for handling PII during telework.

Protecting A-Files at Facilities

USCIS has not performed PIAs to identify privacy threats and ways to mitigate them at service centers and field offices, particularly when A-Files are physically moved from one operation to another or transported among USCIS facilities. The PIA process includes reviewing applicable privacy policies, identifying specific privacy vulnerabilities, and determining ways to mitigate risks at service centers and field offices.

Existing PIAs on USCIS information technology systems that contain PII do not adequately address risks when employees handle A-Files to process immigration benefits and services. According to DHS Privacy Office *Policy Guidance Memorandum 2008-02*, PIAs should be conducted for programs, activities, technologies, and rulemakings, regardless of their type or classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department. PIAs on activities that raise privacy concerns related to the use of PII will ensure greater transparency and help build trust in DHS operations.

A PIA on A-File processing will provide the public with a comprehensive view of the integration of privacy in operations and how privacy concerns have been addressed through USCIS implementation of privacy controls. USCIS Management Directive (MD) 140-001, *Handling Sensitive and Non-Sensitive Personally Identifiable Information*, requires its employees to maintain control over files containing PII. However, during a 2-year period (2008 and 2009), USCIS reported that more than a third (37%) of privacy incidents involved employees' lack of control over A-Files as they pass to subsequent operations or during transportation to other locations.³ In 2009, management

³ The remaining incidents involved information technology issues, such as improper handling of emails containing PII, the loss of removable data devices containing PII, or mailing files to the wrong recipient or facility (109 of 173 incidents, 63%).

reported a monthly average of 257,000 missing A-Files in all facilities.

Improved privacy controls at USCIS facilities will help mitigate the privacy risks that exist as employees handle A-Files to adjudicate benefits and provide services. For example, the four service centers in California, Nebraska, Texas, and Vermont consist of 10 different facilities. Each service center consists of one to four buildings that are located up to 30 miles away from each other. Therefore, within a single service center, employees may move A-Files to different locations as often as 10 times to receive inbound A-Files, temporarily store A-Files, conduct background checks, adjudicate benefits, prepare outbound A-Files, and load A-Files on and off of docks. Figure 3 shows how large volumes of files are handled daily to complete the processing of a particular service or benefit.

Figure 3. Stages of Processing Alien Registration Files Containing Personally Identifiable Information



Source: OIG.

Senior leadership and operations managers have the overall responsibility to ensure that USCIS protects privacy and are accountable for PII contained in A-Files at their service centers and field offices. Until managers assess the processes, flow, and handling of A-Files during specific high-risk operations at facilities, USCIS will continue to expose PII to unmitigated privacy risks.

Telework Needs Specific Privacy Rules of Conduct

USCIS faces challenges in protecting PII that is processed by teleworking employees. Specifically, USCIS has not provided specific instructions, including privacy rules of conduct that are related to handling PII during telework. Presently, the USCIS *Telework Instruction Handbook* (USCIS IHB 123-001) requires teleworkers to ensure that their activities and business processes at the telecommuting site replicate office practices and safeguards that comply with DHS guidance. Presently, USCIS guidance does not provide specific rules of conduct related to the unique risks to handling PII during telework.

The USCIS program has unique challenges because adjudicators who telework must transport extensive amounts of paper A-Files with them to telework sites. The adjudication of benefits requires the review of multiple folders related to the same applicant that can be several feet thick. The contents of an A-File may range from a single page to hundreds of pages that document the history of interaction between USCIS and the applicant. A-Files may include PII, such as submitted benefits and naturalization forms, dates of birth, photographs, fingerprints, and correspondence from family members or third-party sponsors.

On average, an adjudicator at a service center who teleworks four days per week will transport about 2,000 A-Files a year between the office and the telework site. Because the service centers have more than 2,000 adjudicators who are eligible for telework, it is possible that 4 million A-Files will be transported by personal vehicle each year. Figure 4 illustrates the size of A-Files that teleworkers can typically transport.

Figure 4. Examples of Alien Registration Files



Source: OIG.

Missing files are identified in a monthly report that also shows the number of missing files per facility. In 2009, the four service centers averaged more than 27,000 missing A-Files each month by on-site employees and teleworkers. Figure 5 lists the number and percentage of missing A-Files at each of the four service centers and the respective telework participation rates. The two service centers with the highest telework participation rates (24% Texas, 23% Vermont) have 71% (39% Vermont, 32% Texas) of the total missing A-Files.

Figure 5. Service Center Telework Participation/Monthly Missing Alien Registration Files Rates in 2009

MISSING A-FILES BY SERVICE CENTERS		
Service Center	Avg #/ % of Missing Files	Telework Participation Rate
California	3,328 (12%)	7%
Nebraska	4,608 (17%)	17%
Vermont	10,474 (39%)	23%

MISSING A-FILES BY SERVICE CENTERS		
Service Center	Avg #/ % of Missing Files	Telework Participation Rate
Texas	8,713 (32%)	24%
<i>Total</i>	27,123 (100%)	

Source: OIG analysis of monthly USCIS missing files reports in 2009/Telework participation rates.

Greater telework participation increases the risks to PII because teleworkers are transporting more A-Files to additional locations than if the A-Files were processed at the office. However, the *Telework Instruction Handbook* does not provide specific privacy rules of conduct related to telework that could prevent the loss or unauthorized exposure of the content of A-Files. For example, the handbook does not include a procedure on how to secure or recover A-Files prior to and after a car accident while telecommuting. As a result, there have been incidents when documents containing PII were exposed. For example, a teleworker was incapacitated following an automobile accident and unable to protect the PII being transported in the car. In another incident, containers that held A-Files were so damaged by the force of the collision that the files scattered out of the car and across the highway.

If USCIS develops guidance on specific ways to apply privacy rules of conduct for adjudicators who telework that are consistent with DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information*, then risks to PII during telework may be mitigated. Without privacy rules of conduct for teleworkers, employees have insufficient guidance to replicate office practices and safeguards while telecommuting.

Recommendations

We recommend that the Deputy Director of USCIS:

Recommendation #1: Identify vulnerabilities and ways to mitigate privacy risks to A-Files by conducting privacy impact assessments for high-risk operations at service centers and other field facilities.

Recommendation #2: Issue privacy rules of conduct for teleworkers, consistent with DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information*.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Deputy Director of USCIS. A copy of the comments is in Appendix B.

USCIS concurred with our findings and recommendations. Concerning recommendation #1, USCIS is convening an internal working group, led by the Privacy Officer, with appropriate cross-representation of agency operations to prepare a plan of action to mitigate identified weaknesses within 90 days of the findings. Specifically, the working group will focus on privacy stewardship, review all aspects of A-File processing, ensure that file management achieves full privacy compliance, identify and implement business process improvements, and create and oversee implementation of pertinent guidelines and training. In addition, the Records Operations Handbook/Mail Room Operations will be reviewed to ensure consistency with the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information*, and the Office of Security and Integrity/Internal Review Division will update its internal review questionnaire to evaluate compliance with privacy standards. We consider recommendation #1 open, pending our review of documentation that establishes the working group, describes privacy-related plans of action and milestones, and amends USCIS handbooks and the internal compliance questionnaire.

USCIS concurs with recommendation #2. Within 60 days after agreement with the American Federation of Government Employees, USCIS indicated that it will insert appropriate privacy language, consistent with DHS *Handbook for Safeguarding Sensitive Personally Identifiable Information* and DHS 4300A, into its Telework Management Directive and Telework Handbook to ensure that staff are aware of their responsibilities. We consider recommendation #2 open, pending our review of documentation regarding such amendments.

Technical Risks to PII Need to Be Addressed

USCIS has unresolved technical weaknesses that leave PII unprotected in information systems. Specifically, USCIS does not protect PII that is stored on removable data devices adequately. In addition, PII that is sent via email needs better protection. Further, USCIS needs to use system auditing and monitoring to ensure compliance with privacy protection requirements.

Safeguarding Removable Data Devices

USCIS needs to ensure that PII is being protected appropriately when saved on removable data devices. USCIS MD 140-001 prohibits the use of unauthorized removable data devices, such as thumb drives and laptops. According to information security managers at headquarters, they have the ability to detect and disable unauthorized removable data devices on its network. However, information security managers told us that USCIS is not using the detection application because it cannot differentiate devices attached to the network. Instead, the application will disable all attached devices on the network. Further, our testing at several workstations that contained PII at different facilities indicated that the safeguards were not functioning. We were able to connect and use several unauthorized removable data devices.

In addition, USCIS needs to improve the use of encryption to protect PII on removable data devices, as required by OMB M-07-16.⁴ For example, one of the systems we reviewed, the Customer Profile Management System, does not encrypt applicant information before it is transferred to removable data devices. Further, USCIS reported privacy incidents, such as when an employee lost an unencrypted government thumb drive containing PII at a public airport. A civilian recovered and returned the thumb drive to USCIS. Because the data on the thumb drive were unencrypted, anyone could access the PII contained on the device.

Information security managers told us that USCIS is looking into possible solutions to track all removable data devices and to standardize encryption on these devices. Until these solutions are implemented, PII being stored on removable data devices will remain vulnerable to unauthorized disclosure.

⁴ Encryption is the process of using algorithmic schemes that encode plain text into nonreadable form or cyphertext, providing privacy and security of information.

PII in Emails

USCIS employees need to ensure that PII is protected adequately when transmitting it via email. According to DHS *Sensitive Systems Policy Handbook* 4300A, components must consider encryption technologies to protect PII when transmitting it via email. Generally, USCIS employees use various methods to protect PII, such as using a password to protect an email attachment or public key infrastructure, if available.⁵ However, privacy incidents have occurred because these methods have not been used consistently. USCIS reported privacy incidents involving employees who have sent unencrypted emails that contain PII to recipients outside of DHS. During a 2-year period (2008 and 2009), USCIS reported that 71 (41%) of 173 privacy incidents involved unencrypted emails containing PII.⁶

System Auditing and Monitoring

USCIS does not employ auditing and monitoring of systems containing PII to ensure compliance with applicable privacy protection requirements. The DHS Privacy Office *Privacy Technology Implementation Guide* recommends that components audit the actual use of PII and monitor any system with PII. USCIS information security managers told us that existing systems have technical limitations that make auditing and system monitoring not feasible. Instead, they plan to replace existing systems and software with ones that will have auditing and system monitoring capabilities. Meanwhile, important case management systems—such as USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum and USCIS Computer Linked Application Information Management System—do not use system auditing and monitoring. See Appendix E for types of PII maintained within these systems.

Recommendation

We recommend that the Deputy Director of USCIS:

Recommendation #3: Develop plans and milestones for mitigating the technical weaknesses in PII systems regarding

⁵ Public key infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks.

⁶ The remaining incidents involved employees not maintaining control of paper PII files during transportation or employees mailing files to the wrong facility or recipient (80 incidents, 46%) or the loss of removable data devices containing PII (22 incidents, 13%).

removable data devices, encryption, and system auditing and monitoring.

Management Comments and OIG Analysis

USCIS concurs with recommendation #3. The USCIS Chief Information Security Officer has issued written guidance on using or transporting sensitive information in portable storage devices and is working with USCIS Office of Contracting, USCIS Office of Administration's Asset Management Branch, and DHS Efficiency Review Board regarding statements, policies, and tracking of authorized encrypted universal serial bus devices. In the interim, USCIS is researching capabilities to disable use of nonauthorized universal serial bus devices on the network and working with the USCIS Office of Contracting to prevent government purchases of nonauthorized thumb drives. The Chief Information Security Officer will be overseeing full implementation of public key infrastructure by September 2012. In the interim, users are to follow instructions on the agency's Intranet on using WinZip to password protect or encrypt emails and attachments. In addition, USCIS plans to issue a policy on audit and accountability, and implement efforts regarding network monitoring, performance testing, and storing audit logs. We consider recommendation #3 open, pending our review of documentation of such efforts.

Physical Security Standards Need Consistent Enforcement to Protect PII

USCIS employees handle large volumes of PII and often face challenges when safeguarding paper-based PII files and other sensitive information. Physical security addresses perimeter, exterior, and interior measures for securing and protecting PII. These measures should protect buildings and related infrastructure against threats from various sources. However, USCIS has not implemented physical security standards consistently at its facilities to protect PII and other sensitive information.

The Privacy Act requires agencies to establish physical safeguards to protect PII. The DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines on how to protect PII in different physical environments, contexts, and formats, and what to do if PII may have been compromised. Further, according to National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security*, physical security involves access controls that restrict entry and exit of personnel and barriers to isolate areas. Access controls include card key readers, turnstiles, closed-circuit television cameras, motion and intrusion detection, security lighting, perimeter fencing, and contingency planning. Figure 6 shows examples of controls for physical access.

Figure 6. Examples of Controls for Physical Access



Source: OIG.

In 2008, USCIS established a physical security division to address physical safeguards for 249 facilities worldwide to ensure consistency in the application of physical safeguards at each facility. In June 2010, USCIS finalized and posted *Facility Security Standards* on its Intranet site with minimum requirements to protect personnel, property, and assets at all facilities. Our inspections of 22 facilities determined that physical security standards are not consistent with the *Facility Security Standards*. According to officials from the Office of Security and Integrity (OSI) at USCIS headquarters, many facilities are trying to implement the new

physical security standards. OSI has issued a checklist that facilities can use to self-certify compliance with the standards, but many facilities have not filled existing staff vacancies for their security managers to implement the standards. Although OSI staffs are aware that similarly functioning facilities have inconsistently implemented the standards, it has not established how it will verify that standards were implemented properly in each USCIS facility.

Further, our site inspections revealed inconsistencies with the implementation of standards for access controls (e.g., card key readers, closed-circuit television, security lighting, perimeter fencing, restricted parking, contingency planning) used to identify, track, or record authorized personnel, entry, or exit in areas where PII is being transported, handled, or stored. For example:

- **Recording length of closed-circuit television tapes.** The standard requires that closed-circuit television tape recordings be maintained for a minimum of 30 days. However, at several facilities that we inspected, physical security managers maintained tape recordings from 19 days to 60 days.
- **Existence of contingency plans.** The standard requires facilities to maintain contingency plans to ensure continuity of operations. However, according to physical security managers, several facilities either do not have contingency plans or have incomplete plans.

USCIS needs to enforce the consistent implementation of physical security standards to protect PII files throughout its facilities. Inconsistencies in the implementation of standards can result in the loss or disclosure of PII and other sensitive information.

Recommendation

We recommend that the Deputy Director of USCIS:

Recommendation #4: Enforce the consistent implementation of physical security standards.

Management Comments and OIG Analysis

USCIS concurs with recommendation #4. USCIS OSI created a multiyear strategy to update USCIS access control and closed-circuit television systems nationwide. USCIS is assessing physical security countermeasures and policies to protect personnel, property, and assets at headquarters offices adequately. By the end of FY 2011, USCIS plans to address security countermeasures at

field offices and service centers. In addition, to promote consistent access control policy and procedures at USCIS-controlled space and aid implementation across the enterprise, OSI plans to disseminate its draft instructional handbook for review and comment by the end of FY 2011. We consider recommendation #4 open, pending our review of documentation from such efforts.

Privacy Training and Awareness Need Improvement to Increase Effectiveness

The Privacy Act requires agencies to establish appropriate administrative safeguards to protect PII. These safeguards include privacy training and awareness activities. Although USCIS provides required annual refresher privacy training, manager and employee recommendations indicate that improvements are needed.

We conducted a survey of USCIS privacy culture and solicited opinions on how its workforce could improve their understanding of privacy. See Appendix F for survey methodology and results. Sixty-two percent (2,179) of 3,497 written comments by survey respondents related to improvements to privacy training and awareness.

Add Job-Specific, Advanced, or Specialized Privacy Training

OMB M-07-16 requires that privacy-related communications and training be related more specifically to the jobs that employees perform. In addition, OMB promotes advanced or specialized training to improve employees' understanding of their privacy responsibilities in their daily work activities. However, USCIS does not have standardized job-specific, advanced, or specialized privacy training programs to meet the needs of employees.

Overall, survey respondents who provided written comments related to improving job-specific, advanced, or specialized training also offered suggestions on how USCIS could implement privacy safeguards into their daily work. Most suggestions are related to the following five categories 1) developing more training that incorporates privacy on-the-job, 2) integrating more real-world examples where privacy safeguards could be applied, 3) embedding privacy into standard operating procedures, 4) holding more staff briefings on privacy, and 5) increasing opportunities for peer discussions and supervisor mentoring on privacy.

Managers recognize the importance of embedding privacy safeguards in daily work, but they have not assessed their needs or approaches for more job-specific privacy awareness, procedures, or training with their employees. The Office of Privacy recognizes the importance of having job-specific, advanced, and specialized privacy training programs. However, it does not have sufficient resources to identify the specific requirements and needs for

additional training related to the variety of job operations performed by employees.

Implementing the recommendations of managers and employees for job-specific or advanced privacy training can increase the effectiveness of annual privacy training. Specifically, employees will be able to apply broader privacy concepts to their specific jobs. To improve privacy implementation, USCIS will need a collaborative effort among operational managers, supervisors, and program-level experts with assistance from the Office of Privacy to identify requirements for job-specific privacy training. Without a collaborative effort to leverage the limited time and resources of each group in addressing similar needs, employees may interpret or apply privacy protections inconsistently.

Increase Frequency and Vary Methods for Additional Privacy Training

The DHS Privacy Office *Guide to Implementing Privacy* recommends that components employ different methods to deliver privacy training. Also, survey respondents recommended that USCIS increase frequency and vary the methods of delivering additional privacy training through the use of videos, videoconferencing, teleconferencing, and simulations.

USCIS deploys primarily an online computer course for annual privacy training because USCIS has a diverse workforce spread across 250 offices around the world. Although the Office of Privacy provides some instructor-led training for smaller groups at specific locations, this office does not have adequate resources to expand training or employ additional technology to improve the nature and methods of training. However, we observed that some facilities had the capability to use technological enhancements, such as broadcasting in-person training using videoconferencing. Without varying the approach, delivery, and frequency of privacy training, USCIS will not be able to communicate important and timely information to employees in a more meaningful format and approach.

Increase Privacy Awareness Activities

OMB M-07-16 recommends that agencies should augment privacy training by using creative methods to promote daily awareness of the employees' privacy responsibilities. However, according to managers and employees whom we interviewed, USCIS could

improve and increase privacy awareness. Survey respondents suggested specific privacy awareness activities. Examples include weekly privacy tips, privacy email reminders, flyers, banners, wallet-sized cards, and posters.

Figure 7 illustrates posters that heighten the workforce’s awareness that records represent people’s lives and contain personal and confidential information. Similar posters can remind employees about the importance of safeguarding privacy in their daily work.

Figure 7. *Records Are People, People’s Lives*



Source: USCIS Records Division.

Require Privacy Training for Contractors

The DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information and Privacy Incident Handling Guidance* establish privacy responsibilities for both DHS employees and contractors. USCIS MD 140-001 also requires employees and contractors to complete annual privacy training.

USCIS relies on contractors to assist with operations that require the handling of PII, such as file room operations, data entry, and information technology help desk. Although contractors comprise about 40% of the USCIS workforce, existing contracts do not contain requirements for contractor staff to complete annual privacy training. According to USCIS, the intent of these contracts was to maximize productivity. Therefore, they did not consider adding a privacy training requirement to the contractors’ scope of work that would allocate time for training in lieu of production work.

Presently, the Office of Privacy, the Office of Contracting, and the General Counsel are planning to develop privacy training clauses for use in contracts. Without these clauses, USCIS is unable to require contractors to take privacy training. By not enforcing privacy training for these contractors, USCIS is exposing the public's PII to unnecessary risks.

Recommendations

We recommend that the Chief Privacy Officer of USCIS:

Recommendation #5: Implement employee recommendations into plans for privacy training and awareness.

We recommend that the Deputy Director of USCIS:

Recommendation #6: Establish a working group to develop a standardized process to ensure that privacy training clauses are inserted and enforced in contracts related to the handling or maintenance of PII.

Management Comments and OIG Analysis

USCIS concurs with recommendation #5. USCIS has integrated privacy awareness information in current computer security training that emphasizes that all personnel must be able to identify PII and know proper handling guidelines. In addition, USCIS plans to deploy customized privacy training modules for all employees and contractors about 1) privacy fundamentals for the general workforce and 2) targeted training for PII handlers. Also, USCIS scheduled a Privacy Awareness Week that included privacy awareness-building activities, guest speakers, privacy training, and the introduction of a series of one-minute training videos on privacy issues. We consider recommendation #5 open, pending our review of documentation from such efforts.

USCIS concurs with recommendation #6. Through an established working group consisting of the Offices of Privacy, Chief Counsel, and Contracting, USCIS has finalized clauses that mandate PII training for contractors. In addition, USCIS has drafted statements of work for privacy review and determination related to 85 existing contracts and as part of a mandatory privacy review by its Privacy Officer on all new acquisitions over \$100,000. We consider recommendation #6 open, pending our review of documentation of such efforts.

Appendix A

Purpose, Scope, and Methodology

Our objectives were to determine whether plans and activities at USCIS instill and promote a privacy culture and whether it complies with federal privacy laws and regulations. As background for this audit, we researched federal laws and guidance related to responsibilities for privacy protections at USCIS. We reviewed testimonies, documentation, and reports related to USCIS privacy, information technology security, and program management.

We interviewed officials from the DHS Privacy Office, USCIS Office of Privacy, Service Center Operations Directorate, Field Operations Directorate, Refugee, Asylum, and International Operations Directorate, Fraud Detection and National Security Directorate, Customer Service Directorate, Enterprise Services Directorate, Office of Transformation Coordination, and Management Directorate. We interviewed more than 150 program managers, information system, and facility security professionals at headquarters and field sites regarding privacy activities. More than 5,600 federal employees responded to our Privacy Culture survey regarding their opinions on privacy stewardship and knowledge of the *Privacy Act of 1974*, PII handling, and privacy incident response. Of these respondents, 3,497 offered written comments and suggestions on the status, issues, or challenges in privacy stewardship. (See Appendix F.)

We reviewed work production plans, continuity of operations plans, system security documentation, privacy impact assessments, system of records notices, and program-level application of federal privacy laws and guidance. We observed the processes and inspected 22 facilities for the collection, handling, processing, maintenance, and storage of PII. Facilities included the four service centers, National Benefit Center, National Records Center, Western Telephone Center, regional offices, field offices, asylum offices, and application support centers.

We conducted this performance audit between June and December 2010 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 on our audit objectives.

Appendix A
Purpose, Scope, and Methodology

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, Information Technology Audits, and Marj Leaming, Director, System Privacy Division, at (202) 254-4100. Major OIG contributors to the audit are identified in Appendix G.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director (MS 2000)
Washington, DC 20529-2000




**U.S. Citizenship
and Immigration
Services**

APR 29 2011

Memorandum

TO: Frank Deffer
Assistant Inspector General, Information Technology Audits

FROM: Lauren Kielsmeier 
Acting Deputy Director, U.S. Citizenship and Immigration Services

SUBJECT: USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only*
OIG Project No. 10-144-ITA-USCIS

USCIS appreciates the opportunity to review and comment on the subject report.

Recommendation #1: Identify vulnerabilities and ways to mitigate privacy risks to A-files by conducting privacy impact assessments for high risk operations at service centers and other field activities.

USCIS's Response: USCIS concurs with this recommendation. The report notes that during the period of review (2008 and 2009) 37% of privacy incidents involved employees' lack of control over A-files as the files passed through subsequent operations or during transport. USCIS's current operations require the creation and use of paper Alien Registration Files (referred to as A-files) throughout the adjudication process. The files are manually transported to various offices depending on the level and extent of adjudication required. The USCIS Office of Privacy notes that the majority of the incidents cited in the report were the result of external errors outside the control of USCIS employees (e.g., courier incidents). However, any privacy incident is unacceptable and USCIS recognizes the need to implement processes and procedures to minimize the possibility of such incidents occurring. The following paragraphs discuss the actions taken to address this recommendation.

USCIS will establish a working group led by the Privacy Officer and consisting of representatives from USCIS Programs and Directorates to review the handling and movement of A-files across the agency. The working group will review all aspects of file processing at USCIS to ensure full compliance with all pertinent regulations that address file management. Additionally, the group will focus on Privacy Stewardship. The working group will identify and implement improvements in business processes and oversee the refinement, creation and dissemination (to include training) of implementing guidelines and directives to all USCIS personnel.

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 2

At present, the Records Operations Handbook (ROH) describes Mail Room Operations at USCIS (i.e., how files are received and moved at USCIS), in addition to the creation, storage, and tracking of all files. The ROH is an enduring handbook that is regularly reviewed to ensure accuracy and consistency with operational procedures. The ROH will be further reviewed and amended to ensure it discusses policy and provides guidance consistent with the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (PII).

In 2007, the USCIS Office of Security and Integrity (OSI), Internal Review Division developed an internal review questionnaire to evaluate the Records Program at USCIS file control offices. OSI works with the Records Division to ensure that the questionnaire is updated on a regular basis to reflect current records policy. OSI will update the questionnaire to ensure that in the future we evaluate compliance with privacy standards. This process will help USCIS determine internal weaknesses and facilitate a process to mitigate those weaknesses via training and policy changes.

As part of its Transformation Program, USCIS is further mitigating this risk by transitioning to the Integrated Operating Environment (IOE). In the IOE, USCIS will not have to physically transport the files between facilities, because the relevant files will be available through the IOE's secure online environment. As the IOE is implemented, the number of files requiring physical transport will gradually decrease, because *new* benefit seekers will only have online files. USCIS employees (including those on telework) will simply log in to the IOE, rather than carrying files to and from their homes.

USCIS believes an alternative approach to conducting privacy impact assessments should be utilized in identifying and assessing high risk operations at service centers and other field activities. USCIS recommends convening an internal working group with appropriate cross-representation from agency operations as a more feasible approach. USCIS Executive Leadership would establish the working group to identify potential weaknesses and establish a plan of action and milestones for mitigating the findings. USCIS anticipates establishing a working group within 90 days of this response. USCIS also plans to identify weaknesses and potential mitigation to each weakness, 90 days from the findings.

Recommendation #2: Issue privacy rules of conduct for teleworkers, consistent with DHS Privacy Office: Handbook for Safeguarding Sensitive Personally Identifiable Information.

USCIS's response: USCIS concurs with this recommendation. The OIG review identifies the unique challenges to privacy stewardship with respect to Telework and focuses on USCIS Service Centers; however, it should be noted at the time DHS (and USCIS) was established in 2003, telework was already in place as a pilot program at the USCIS Service Centers. The removal of A-files to alternate worksites was an established work practice at USCIS Service Centers. The USCIS Telework MD was actually finalized in January 2009 after USCIS completed its negotiations with the American Federation of Government Employees (AFGE). USCIS will insert the appropriate language in the Telework MD to ensure staff is aware of their

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 3

responsibility to properly secure and protect PII at all times. The Telework MD revision will ensure USCIS' Telework Program conforms to the "DHS Handbook for Safeguarding Sensitive PII" and DHS Directive 4300A, "Sensitive Systems Policy." Once the revised MD is prepared, USCIS will work with AFGE to obtain their agreement on the revisions. USCIS will also amend its Telework Handbook to ensure consistency with USCIS MD and the DHS handbook. The amendment to the Telework MD will be accomplished within 60 days after an agreement is reached with the Bargaining Unit.

Once USCIS deploys the IOE, the need for telework personnel to transport files will gradually diminish. The IOE's collaborative referral and case management capabilities will provide a secure alternative to emailing PII.

Recommendation #3: Develop plans and milestones for mitigating the technical weaknesses in PII systems regarding removable data devices, encryption and system auditing and monitoring.

USCIS's response: USCIS concurs with this recommendation. The Office of Information Technology (OIT) has initiated the deployment of Public Key Infrastructure (PKI) certificates agency-wide. The Chief Information Security Officer (CISO) is overseeing the implementation of the PKI and the goal is to have certificates issued to 40% of all USCIS employees by September 2011 and the remaining 60% by September 2012. The PKI certificates integrate with the agency's e-mail system so users can encrypt emails and attachments. In the interim, users are instructed to password protect or encrypt attachments using WinZip. Instructions on the use of WinZip are posted on the agency's intranet.

To ensure compliance with privacy standards when utilizing thumb drives, OIT is currently working on the following activities:

- Researching the capabilities of McAfee ePolicy Orchestrator and Windows 2007 software to disable the use of non-authorized USB devices on the network.
- Working with the Office of Contracting to develop a process to prevent the purchase of non-authorized thumb drives on Agency Purchasing Cards.
- Working on the identification and removal of all thumb drives that do not have encryption capability or do not comply with FIPS 140-2 encryption standards.
- Working with the Office of Administration's Asset Management Branch to ensure all government purchased thumb drives are imprinted with a unique identification number and tracked in the Agency's Asset Management System.
- Participating on the DHS Efficiency Review Board to finalize the DHS Statement of Work (SOW) for the acquisition of Encrypted USB Devices.
- Issuing a USCIS policy memorandum on the use of portable USB storage devices on the network.

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 4

On January 25, 2011, the CISO issued written guidance on the use of portable storage devices. The CISO's guidance provides information on properly transporting information in electronic form and instructs personnel to adhere to DHS MD 11047, "Protection of Classified National Security Information Transmission and Transportation," and DHS MD 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information" when transporting sensitive information in paper form.

OIT is currently working on the following activities concerning the auditing and monitoring of USCIS information systems:

- Drafting the USCIS Audit and Accountability MD; this policy will mandate the configuration of all USCIS information systems to record all user actions within the system. It will also require PII systems to connect to the enterprise audit log comparison tool. The MD is scheduled to be released by September 30, 2011.
- Implementing a network monitoring tool to integrate legacy information systems with the enterprise audit log comparison tool.
- Conducting performance testing on one of the case management systems to ensure the use of the monitoring tools does not impede application performance.
- Identifying available storage locations for case management system's audit logs.

Recommendation #4: Enforce the consistent implementation of physical security standards.

USCIS's response: USCIS concurs with this recommendation. USCIS employs physical security standards across the enterprise; the most recent achievement was the implementation of USCIS IHB 121-01-601, "Facility Security Standards (FSS)" in June 2010. Using the USCIS Physical Security Inspection Workbook (based on standards outlined in the FSS), OSI is assessing USCIS Headquarters (HQ) offices to determine if the building infrastructure and security countermeasures adequately protect USCIS personnel, property, and assets. USCIS will implement physical security countermeasures and policies based on each facility's unique operating environment. OSI will begin assessing field offices and service centers during the latter part of fiscal year 2011.

In addition to assessing security countermeasures at field offices and service centers, OSI created the Electronic Security Systems (ESS) Nationwide Deployment Project in September 2010. ESS is an element of OSI's Homeland Security Presidential Directive 12 (HSPD-12) implementation plan and its primary focus is to update USCIS access control systems to meet Federal Information Processing Standards (FIPS) 201 and HSPD-12 standards. The ESS Project is a multiyear strategy that will integrate, standardize and upgrade or replace many USCIS access control and CCTV systems nationwide.

It is important to note that USCIS primarily occupies multi-tenant facilities nationwide. In a multi-tenant facility, a USCIS representative is a member of the Facility Security Committee (FSC). Each FSC, which is made up of tenants in the facility, considers and makes decisions on

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 5

facility security matters to include physical access/entry control (into the facility – not into tenant workspace), contract guard staffing, screening procedures, and other facility security measures. Because USCIS resides in a variety of facilities (e.g., multi-tenant, high-rise or multi-story) with varying Facility Security Levels (FSLs) physical security countermeasures and policies will vary between facilities.

The subject report cites the inconsistent application of access control systems and other supplementary security countermeasures that are used to mitigate potential threats to personnel in areas where PII is being transported, handled, or stored. Specifically, the report expands on the following:

- Recording Length of Closed-Circuit Television Tapes
- Adequate External Security Lighting
- Adequate Application of Perimeter Barriers
- Adjacent Surface Parking Distances
- Existence of Contingency Plans

As mentioned, USCIS implements physical security countermeasures and policies based on each facility's unique operating environment—each facility's unique situation dictates the feasibility and availability of security countermeasures. For example, there are three major factors that play a role in the application of perimeter barriers:

- 1) The availability of real estate to support the countermeasure. Fixed in-ground bollards may not be installed in some areas because the ground is too fragile and unable to support the weight of the materials.
- 2) Local city/municipality, county, or state planning commissions may not allow the Federal government to place perimeter barriers around its facilities. Many local governments explain that barriers are not aesthetically pleasing to the eye.
- 3) USCIS receives security risk assessments from the Federal Protective Service (FPS) that identify potential threats to the facility and its personnel and assets. Barriers are not installed if it is determined that the level of threat to the agency does not warrant the installation of the countermeasure.

Essentially, the FSS provides a minimum level of protection in its application of perimeter barriers at USCIS facilities; however, the level of protection can be customized once the risks have been identified and all parties (with decision making authority) agree that the risk does or does not warrant the countermeasure.

Lastly, another step toward standardization resides in the implementation of written policy and procedures. OSI has a draft instructional handbook (IHB) that promotes consistent access control policy and procedures at USCIS controlled space: USCIS IHB 121-01-632, USCIS Headquarters Access Control. The USCIS HQ Access Control IHB will be disseminated to

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 6

stakeholders for review and comment with a tentative implementation date of 4th Quarter FY11. Field offices will be advised to utilize the USCIS HQ Access Control IHB as a model/template to implement consistent access control policy across the enterprise with the understanding that some access control procedures/measures must be tailored specifically to their unique operating environment. This draft IHB will bridge the gap in overarching access control policy and procedures while awaiting DHS Department-wide access control policy

Recommendation #5: Implement employee recommendations into plans for privacy training and awareness.

USCIS's response: USCIS concurs with this recommendation. USCIS had previously taken some steps to implement employee recommendations into instructor-led training. These include: presenting real-world examples of common types of PII/data security breaches USCIS experiences and how they were mitigated; clarifying USCIS policy on transmission of PII via email (subsequently, as a result, the USCIS Privacy Officer issued additional guidance), and increasing the variety of privacy training utilizing multiple forms of delivery including computer-based, instructor-led (both in-person and via webinar), videos, and relying on the USCIS Office of Privacy's intranet web page. USCIS will continue to implement employee recommendations into privacy training and awareness activities.

In FY 2011 USCIS will deploy two new custom privacy awareness training modules which integrate multiple-choice, true/false, case studies, and scenario-based questions, and utilize the latest in training technology. All USCIS employees and contractors will be required to complete the training annually. One training module is targeted to the general workforce and covers privacy fundamentals, DHS/USCIS privacy policy, and other privacy requirements as mandated by the Privacy Act. Consistent with OMB Memorandum 07-16, "Safeguarding Against and Responding to a Breach of Personally Identifiable Information", the second training module is targeted to USCIS system business owners, program and system managers, and others whose job responsibilities require more frequent access or use of PII. USCIS will also develop a series of short one-minute training videos on privacy issues. These training videos will enable USCIS to increase the frequency of privacy training, implement more privacy awareness activities, and develop technologically enhanced methods of training. These training videos can also be designed to be job-specific as recommended. USCIS plans to launch these videos during Privacy Awareness Week. Additionally, OIT includes privacy awareness information in their computer security awareness training activities. OIT's training emphasizes the USCIS Rules of Behavior which stipulate that all personnel must be able to identify PII and know the proper PII handling guidelines in accordance with the Office of Privacy's policies and procedures.

While USCIS has made significant progress towards implementing employee recommendations into privacy training and awareness—we plan to do more. Privacy Awareness Week is scheduled the week of April 4, 2011 and will include a variety of guest speakers from the Federal privacy arena, opening and closing remarks from the USCIS Director and DHS Chief Privacy

- For Official Use Only -

Appendix B Management Comments to the Draft Report

- For Official Use Only -

USCIS Response to OIG Recommendations re *USCIS Privacy Stewardship – For Official Use Only/OIG Project No. 10-144-ITA-USCIS*
Page 7

Officer and two days of privacy training, along with awareness-building activities targeted to USCIS employees and contractors.

Recommendation 6: Establish a working group to develop a standardized process to ensure that privacy training clauses are inserted and enforced in contracts related to the handling or maintenance of personally identifiable information.

USCIS's response: USCIS concurs with this recommendation. USCIS established a working group in November 2010 that consists of the Offices' of Privacy, Chief Counsel and Contracting to develop the required contract clauses and to assess current contracts for modification.

The working group has accomplished the following:

- Finalized the necessary contract clauses that mandate PII training for contractor personnel;
- Provided the SOWs for all relevant active contracts to the USCIS Privacy Officer for review and determination on whether PII training is required;
- Identified a total of 85 contracts requiring modification based on the SOW review by the USCIS Privacy Officer and determination that PII Training should be required;
- Completed 75 contract modification and a remaining 10 modifications are pending; and
- Instituted a mandatory review by the USCIS Privacy Officer on all new acquisitions >\$100,000 to ensure future contract fully comply with privacy standards and training requirements.

USCIS is firmly committed to ensuring it fulfills its obligation to create and maintain a robust privacy program. As noted in the subject report, USCIS established its privacy office and designated a Privacy Officer in November 2007 to oversee and manage all aspects of the USCIS privacy program. The USCIS privacy office is committed to working with all of the organizations within USCIS to ensure we have a comprehensive privacy awareness program that includes proper oversight, management and training to ensure full compliance with federal policy and procedures.

- For Official Use Only -

Appendix C

Legislation, Memoranda, Directives, and Guidance Pertinent to the USCIS Privacy Stewardship Audit

LEGISLATION

Privacy Act of 1974, 5 U.S.C. § 552a (2004). <http://www.opm.gov/feddata/USC552a.txt>

E-Government Act of 2002, Public Law 107-347, 116 STAT. 2899 (2002).
<http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

Federal Information Security Management Act of 2002, 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>

Immigration and Nationality Act, Public Law No. 111-306, 8 U.S.C. 1101 (2010).
<http://www.uscis.gov/portal/site/uscis/menuitem.f6da51a2342135be7e9d7a10e0dc91a0/?vgnnextoid=fa7e539dc4bed010VgnVCM1000000ecd190aRCRD&vgnnextchannel=fa7e539dc4bed010VgnVCM1000000ecd190aRCRD&CH=act>

OMB M-02-01: *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (October 17, 2001).
http://www.whitehouse.gov/omb/memoranda_m02-01

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>

OMB M-10-15: *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (April 21, 2010). http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

DHS Memorandum: *Designation of Component Privacy Officers* (June 5, 2009). (No External Link Available)

DHS Privacy Office: *Policy Guidance Memorandum Number 2007-01; DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* (January 7, 2009).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

DHS Privacy Office: *Policy Guidance Memorandum Number 2008-02; DHS Privacy Policy Regarding Privacy Impact Assessments* (December 30, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

DHS Privacy Office: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security* (October 31, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf

DHS Privacy Office: *Guide to Implementing Privacy* (June 2010).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_implementation_guide_june2010.pdf

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

DHS Privacy Office: *Privacy Technology Implementation Guide* (August 16, 2007).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

DHS Privacy Office: *Privacy Impact Assessments Official Guidance* (May 2007).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf

DHS Privacy Office: *Privacy Act Statement Guidance* (April 2008).
[http://dhsconnect.dhs.gov/uscis/org/PVY/Official%20Guidance/Privacy%20Act%20\(E3\)%20Statement%20Official%20Guidance.pdf](http://dhsconnect.dhs.gov/uscis/org/PVY/Official%20Guidance/Privacy%20Act%20(E3)%20Statement%20Official%20Guidance.pdf)

DHS Privacy Office: *System of Records Notices Official Guidance* (April 2008).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf

DHS 4300A: *Sensitive Systems Handbook Version 7.1* (August 9, 2010). (No External Link Available)

Appendix C

Legislation, Memoranda, Directives, and Guidance Pertinent to the USCIS Privacy Stewardship Audit

DIRECTIVES AND GUIDANCE

National Institute of Standards and Technology Special Publication 800-12: *An Introduction to Computer Security: The NIST Handbook* (October 1995). <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

National Institute of Standards and Technology Special Publication 800-21: *2nd Edition: Guideline for Implementing Cryptography in the Federal Government* (December 2005). http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

National Institute of Standards and Technology Special Publication 800-32: *Introduction to Public Key Technology and the Federal PKI Infrastructure* (February 26, 2001). <http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>

National Institute of Standards and Technology Special Publication 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information* (April 2010). <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

USCIS Management Directive 140-001: *Handling Sensitive and Non-Sensitive Personally Identifiable Information* (September 7, 2010). (No External Link Available)

Appendix D
Component Level Privacy Office Designation and Duties

COMPONENTS TO DESIGNATE PRIVACY OFFICERS
<ul style="list-style-type: none"> ▪ U.S. Citizenship and Immigration Services ▪ Federal Emergency Management Agency ▪ National Protection and Programs Directorate ▪ Office of Intelligence and Analysis ▪ Science and Technology Directorate ▪ Transportation Security Administration ▪ United States Coast Guard ▪ U.S. Immigration and Customs Enforcement ▪ U.S. Customs and Border Protection ▪ United States Secret Service
Communicate the component privacy initiatives, both internally and externally.
Monitor component's compliance with all federal privacy laws and regulations; implement corrective, remedial, and preventative actions; and notify the DHS Privacy Office of privacy issues or noncompliance when necessary.
Implement and monitor privacy training for employees and contractors.
Assist in drafting and reviewing Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs), and Systems of Records Notices (SORNs), as well as any associated privacy compliance documentation.
Serve as the point of contact to handle privacy incident response responsibilities as defined in the <i>Privacy Incident Handling Guidance</i> .
Provide privacy information to the DHS Privacy Office for the quarterly <i>Federal Information Security Management Act</i> reporting, Section 803 of the <i>Implementing Recommendations of the 9/11 Commission Act</i> reporting, the DHS Privacy Office Annual Report, and other reporting requirements, as needed.

Source: DHS Memorandum, *Designation of Component Privacy Officers*, June 5, 2009.

Appendix E

USCIS Systems: Privacy Impact Assessments and System of Records Notices

NAME AND PII COLLECTED	PRIVACY IMPACT ASSESSMENT	SYSTEM OF RECORDS NOTICE
<p>Immigration Benefits Background Check Systems (IBBCS) collects biometric information from petitioners who seek certain immigration benefits. Applicants provide biometric information for the FBI Fingerprint Check and the Automated Biometric Identification System Fingerprint Check.</p>	<p>Immigration Benefits Background Check Systems (IBBCS), November 5, 2010</p>	<p>DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS), October 31, 2008, 72 FR 1755 DHS/USCIS-002 - Background Check Service, June 5, 2007, 72 FR 31082 DHS/USCIS-003 - Biometric Storage System, April 6, 2007, 72 FR 1717</p>
<p>National File Tracking System (NFTS) collects and maintains PII pertaining to the applicant, system user, and immigration file.</p>	<p>National File Tracking System (NFTS), October 5, 2010</p>	<p>DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS), January 16, 2007, 72 FR 1755</p>
<p>Citizenship and Immigration Data Repository (CIDR) collects PII directly from and about immigrants and nonimmigrants through applications and petitions for the purposes of adjudicating and providing immigration benefits.</p>	<p>Citizenship and Immigration Data Repository (CIDR), September 8, 2010</p>	<p>DHS/USCIS-012 - Citizenship and Immigration Data Repository (CIDR), September 8, 2010, 75 FR 5464</p>
<p>E-Verify Program: Use of Commercial Data for Employer Verification collects business information from employers and a commercial data provider, Dun and Bradstreet, to verify that registering companies are genuine businesses.</p>	<p>E-Verify Program: Use of Commercial Data for Employer Verification, June 2, 2010</p>	<p>DHS/USCIS-011 - E-Verify Program, May 19, 2010, 75 FR 28035</p>
<p>Customer Identity Verification (CIV) System Update collects and uses PII when an applicant appears before USCIS in person at the time of an interview so that USCIS can verify that the individual being interviewed is the same person for whom it conducted a background check.</p>	<p>Customer Identity Verification (CIV) System Update, April 26, 2010</p>	<p>DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS), January 16, 2007, 72 FR 1755 DHS/USVISIT-0012 - DHS Automated Biometric Identification System (IDENT), June 5, 2007, 72 FR 31080</p>
<p>Eligibility Risk and Fraud Assessment Testing Environment (EFRA) uses synthetic data from different datasets in Treasury Enforcement Communications System.</p>	<p>Eligibility Risk and Fraud Assessment Testing Environment (EFRA), April 9, 2010</p>	<p>DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS), January 16, 2007, 72 FR 1755 DHS/USCIS-007 - Benefits Information System, September 29, 2008, 73 FR 56596 DHS/USCIS-010 - Asylum Information and Pre-Screening, January 5, 2010, 75 FR 409</p>
<p>Background Vetting Service (BVS) facilitates fingerprint checks of U.S. citizens, whose principal residence is overseas, and who is filing family-based immigration petitions at Department of State Overseas Posts.</p>	<p>Background Vetting Service (BVS), March 22, 2010</p>	<p>DHS/USCIS-005 - Inter-Country Adoptions Security, June 5, 2007, 72 FR 31086 DHS/USCIS-007 - Benefits Information System, September 29, 2008, 73 FR 56596</p>
<p>Refugees, Asylum, and Parole System and the Asylum Pre-Screening System collects PII from asylum applicants and applicants for benefits provided by Section 203 of the <i>Nicaraguan Adjustment and Central American Relief Act</i> (NACARA § 203).</p>	<p>Refugees, Asylum, and Parole System and the Asylum Pre-Screening System, November 24, 2009</p>	<p>DHS/USCIS-010 - Asylum Information and Pre-Screening, January 5, 2010, 75 FR 409</p>
<p>Travel and Employment Authorization Listings (TEAL) collects applicant's PII for determining benefit eligibility.</p>	<p>Travel and Employment Authorization Listings (TEAL), November 3, 2009</p>	<p>DHS/USCIS-007 - Benefits Information System, September 29, 2008, 73 FR 56596</p>
<p>USCIS Customer Relationship Interface System (CRIS) Update receives PII from customers over the internet or over the phone.</p>	<p>USCIS Customer Relationship Interface System (CRIS) Update, September 22, 2009</p>	<p>DHS/USCIS-007 - Benefits Information System, September 29, 2008, 73 FR 56596</p>

Appendix E

USCIS Systems: Privacy Impact Assessments and System of Records Notices

NAME AND PII COLLECTED	PRIVACY IMPACT ASSESSMENT	SYSTEM OF RECORDS NOTICE
Reengineered Naturalization Casework System (RNACS) collects applicant's PII at a USCIS Application Support Center (ASC) to conduct background checks.	Reengineered Naturalization Casework System (RNACS) , August 24, 2009	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 565966596
Electronic Filing System (e-Filing) collects PII from applicants based on the specific form(s) selected from a menu of available applications.	Electronic Filing System (e-Filing) , August 24, 2009	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR) replicates the PII to consolidate the data and streamline the process for reporting and information sharing initiatives.	Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR) , August 24, 2009	DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755 DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Compliance Tracking and Management System (CTMS) contains PII on four categories of individuals (any of whom may be either U.S. citizens or non-U.S. citizens): Verification Subjects, E-Verify or Systematic Alien Verification for Entitlements Program Users, Complainants, and DHS Employees.	Compliance Tracking and Management System (CTMS) , May 22, 2009	DHS/USCIS-009 - Compliance Tracking and Monitoring System , May 22, 2009, 74 FR 24022
Correspondence Handling and Management Planning System (CHAMPS) collects and uses PII to process N-400, N-600, and N-565 applications.	Correspondence Handling and Management Planning System (CHAMPS) , January 13, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Changes to Requirements Affecting H-2A Nonimmigrants and Changes to Requirements Affecting H-2B Nonimmigrants and Employers Final Rules collects PII from employers who may collect information from the nonimmigrant workers regarding H-2A and H-2B petitions.	Changes to Requirements Affecting H-2A Nonimmigrants and Changes to Requirements Affecting H-2B Nonimmigrants and Employers Final Rules , December 18, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Scheduling and Notification of Applicants for Processing (SNAP) collects and stores PII provided at the time the USCIS Service Center/National Benefits Center schedules the appointment.	Scheduling and Notification of Applicants for Processing (SNAP) , December 15, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Verification Information System Update collects and verifies U.S. Passport and Passport Card data, which when required for secondary verification purposes may include photographs from employees who present a U.S. Passport or Passport Card as a Form I-9 List A document to an E-Verify participating employer.	Verification Information System Update , November 20, 2008	DHS/USCIS-004 - Verification Information System , December 11, 2008, 73 FR 75445
USCIS Person Centric Query Service Supporting Visa Benefit Adjudicators, Visa Fraud Officers, and Consular Officers of the Department of State, Bureau of Consular Affairs allows users to submit a single query for all transactions involving an immigrant across a number of systems, and returns a consolidated and correlated view of the immigrant's past interactions with the government as he or she passed through the U.S. immigration system.	USCIS Person Centric Query Service Supporting Visa Benefit Adjudicators, Visa Fraud Officers, and Consular Officers of the Department of State, Bureau of Consular Affairs , November 5, 2008	DHS/USCIS-003 - Biometric Storage System , April 6, 2007, 72 FR 17172 DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596 DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755
Alien Change of Address Card (AR-11) contains PII submitted by customers whose addresses have changed during their stay in the United States.	Alien Change of Address Card (AR-11) , October 21, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
DHS/UKvisas Project collects biometrics from applicants at the time of biometric capture at an ASC.	DHS/UKvisas Project , November 14, 2007	No System of Records listed.

Appendix E

USCIS Systems: Privacy Impact Assessments and System of Records Notices

NAME AND PII COLLECTED	PRIVACY IMPACT ASSESSMENT	SYSTEM OF RECORDS NOTICE
USCIS Microfilm Digitization Application System (MiDAS) contains approximately 85 million historic digitally indexed immigration-related records that were previously stored on microfilm. The objective of MiDAS is to enable USCIS personnel to search, retrieve, and deliver PII about individuals contained in USCIS records based on requests received from customers, such as federal, state, and local government agencies and the public.	USCIS Microfilm Digitization Application System (MiDAS) , September 15, 2008	DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755
USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) contains data entered from all CIS customer immigration application forms and petitions except naturalization, refugees and asylum.	USCIS Benefits Processing of Applicants other than Petitions for Naturalization, Refugee Status, and Asylum (CLAIMS 3) , September 5, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
USCIS Computer Linked Application Information Management System (CLAIMS 4) contains data entered from the N-400, Application for Naturalization, as well as data generated by DHS or the FBI.	USCIS Computer Linked Application Information Management System (CLAIMS 4) , September 5, 2008	DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
USCIS Fraud Detection and National Security Data System (FDNS-DS) contains PII collected throughout the following processes: administrative investigations, fraud investigations, adjudication processes, and benefit fraud assessments.	USCIS Fraud Detection and National Security Data System (FDNS-DS) , July 29, 2008	DHS/USCIS-006 - Fraud Detection and National Security Data System (FDNS-DS) , August 18, 2008, 73 FR 48231
USCIS Secure Information Management Service (SIMS) Pilot with Inter-Country Adoptions Update collects and shares PII regarding adoptions with Department of State.	USCIS Secure Information Management Service (SIMS) Pilot with Inter-Country Adoptions Update , August 13, 2008	DHS/USCIS-005 - Inter-Country Adoptions Security , June 5, 2007, 72 FR 31086
USCIS Central Index System (CIS) collects PII directly from the individual requesting benefits under the <i>Immigration and Nationality Act</i> .	USCIS Central Index System (CIS) , June 22, 2007	DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755
USCIS Enterprise Service Bus (ESB) collects operational data used for authentication, authorization, and determination of permissions for a user or system connecting to a deployed service.	USCIS Enterprise Service Bus (ESB) , June 22, 2007	DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) , September 29, 2009, 74 FR 49882
USCIS Biometric Storage System (BSS) collects biometric and associated biographic data provided at the time of biometric capture at an ASC.	USCIS Biometric Storage System (BSS) , March 28, 2007	DHS/USCIS-003 - Biometric Storage System , April 6, 2007, 72 FR 17172
USCIS Naturalization Redesign Test Pilot (NRTP) collects PII from all people interviewed for naturalization at 10 USCIS district offices with appointments from approximately February 15, 2007 through May 15, 2007.	USCIS Naturalization Redesign Test Pilot (NRTP) , January 12, 2007	DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755 DHS/USCIS-007 - Benefits Information System , September 29, 2008, 73 FR 56596
Migrant Information Tracking System (MITS) collects biographic information from the migrant, to include name, date of birth, address, gender, marital status, race, and occupation.	Migrant Information Tracking System (MITS) , February 3, 2011	No System of Records listed.
Integrated Digitization Document Management Program (IDDMP) does not collect new data directly from individuals; rather IDDMP digitizes the hardcopy A-File data collected originally from or on individuals covered by provisions of the <i>Immigration and Nationality Act</i> .	Integrated Digitization Document Management Program (IDDMP) , January 5, 2007	DHS/USCIS-001 - Alien File (A-File) and Central Index System (CIS) , January 16, 2007, 72 FR 1755

Appendix E

USCIS Systems: Privacy Impact Assessments and System of Records Notices

NAME AND PII COLLECTED	PRIVACY IMPACT ASSESSMENT	SYSTEM OF RECORDS NOTICE
<p>H-1B Visa Cap Registration requires the following PII from petitioners and beneficiaries: name, employer identification number, contact information, date of birth, country of birth, country of citizenship, gender, passport number, and any additional information requested by the registration or USCIS.</p>	<p>H-1B Visa Cap Registration, January 28, 2011</p>	<p>No System of Records listed.</p>
<p>E-Verify Self Check collects the individual's name, address of residence, date of birth, and optionally, the individual's Social Security number. Based on citizenship status and the document chosen to present for work authorization, the system collects additional information that can include: citizenship status, Alien Number (if noncitizen), passport number, Form I-94 number, lawful permanent resident card, or work authorization document number.</p>	<p>E-Verify Self Check, March 4, 2011</p>	<p>DHS/USCIS-013 - E-Verify Self Check, February 16, 2011, 76 FR 9034</p>

Source: The DHS Privacy Office has USCIS Privacy Impact Assessments and System of Records Notices at http://www.dhs.gov/files/publications/gc_1279308495679.shtm#content (accessed May 6, 2011).

Appendix F
OIG Privacy Culture Survey

OIG developed a privacy survey with involvement of the USCIS Office of Privacy. The purposes of the survey were to assess the level of workforce understanding of privacy and to obtain recommendations for improvements, based on the criteria in Appendix C.

In July 2010, OIG emailed a link to the USCIS workforce to complete the online privacy survey on a secure site. Survey participation was voluntary, confidential, and accessible only by OIG. The results of the survey were useful because they provided insights into areas in which improvements are needed. The following chart shows the levels of job responsibility, location, and lengths of services for respondents who either completed the survey or provided selected responses.

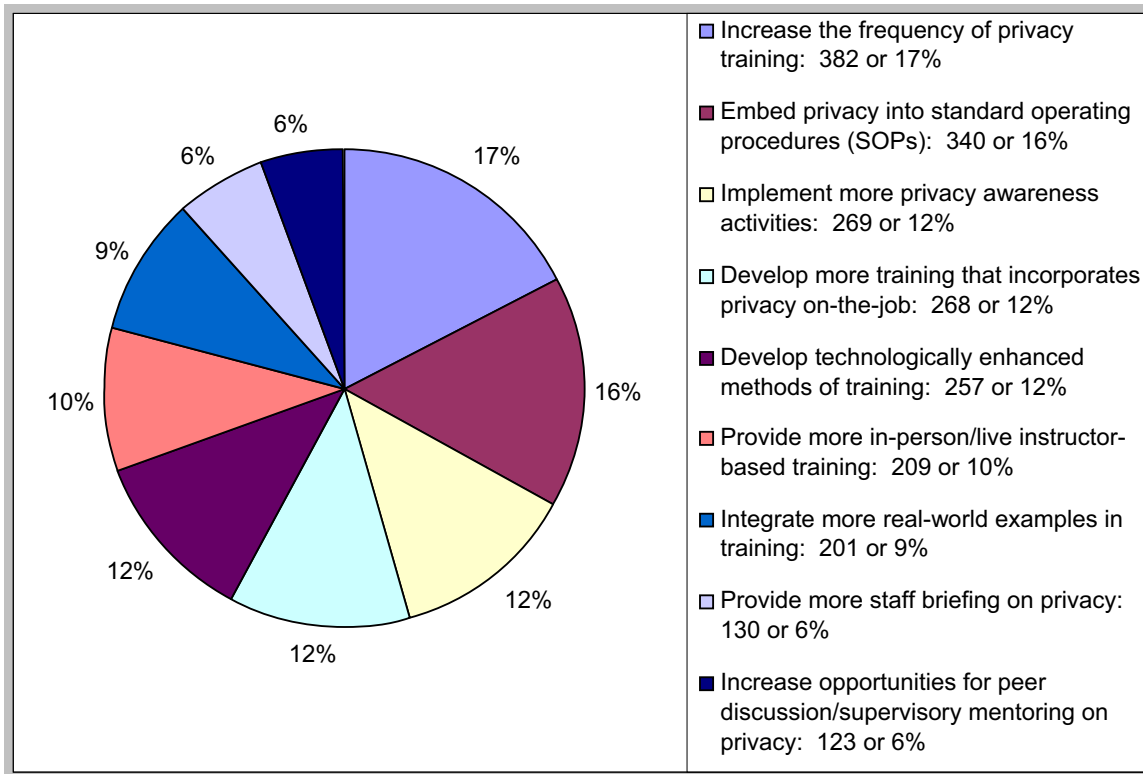
DEMOGRAPHICS OF PARTICIPANTS	
Level of Job Responsibility	
	Entry-level employees (14.4%)
	Mid to high-level (non-manager) employees (66.2%)
	Supervisors/managers (19.4%)
Location	
	Headquarters (17.8%)
	Field - Northeast (23.1%)
	Field - Southeast (9.4%)
	Field - Central (27.3%)
	Field - West (22.4%)
Length of Service	
	Less than 3 months (1.5%)
	3–12 months (4.8%)
	1–3 years (25.3%)
	More than 3 years (68.4%)

Source: OIG Privacy Culture Survey

Of the total 6,915 respondents, 81% (5,602) completed the survey and 19% (1,313) provided selected responses. The completed survey response rate of federal employees was 54% (5,602 of 10,367). We received 3,497 written comments by survey respondents, 2,179 of whom (62%) recommended improvements to privacy training and awareness and 1,318 of whom (38%) commented on the lack of privacy protections in their daily work.

Respondents recommended the following improvements to privacy training and awareness 1) increase the frequency of privacy training (382 or 17%), 2) embed privacy into standard operating procedures (340 or 16%), 3) implement more privacy awareness activities (269 or 12%), 4) develop more training that incorporates privacy on-the-job (268 or 12%), 5) develop technologically enhanced methods of training (257 or 12%), 6) provide more in-person or live instructor-based training (209 or 10%), 7) integrate more real-world examples in training (201 or 9%), 8) provide more staff briefings on privacy (130 or 6%), and 9) increase opportunities for peer discussion and supervisory mentoring on privacy (123 or 6%). The following chart shows the improvements that survey respondents recommended.

Appendix F
OIG Privacy Culture Survey



Source: OIG Privacy Culture Survey, written comments, *N* = 3,497.

Appendix G
Major Contributors to this Report

System Privacy Division

Marj P. Leaming, Director
Eun Suk Lee, Lead Privacy Auditor
Pamela J. Chambliss-Williams, Senior Program Analyst
Hung Huynh, Privacy Specialist
Kevin Mullinix, Management and Program Assistant
Steven Tseng, Management and Program Assistant

Craig Adelman, Referencer

Appendix H

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
Director of USCIS
DHS Privacy Office
USCIS Audit Liaison Office
USCIS Office of Privacy

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.