



Department of Homeland Security Office of Inspector General

Immigration and Customs Enforcement Privacy Stewardship



OIG-10-100

July 2010



Homeland
Security

July 6, 2010

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 Immigration and Customs Enforcement's plans and activities to instill a privacy culture that protects sensitive personally identifiable information and ensure compliance with federal privacy 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 cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	4
ICE Has Made Progress in Privacy Stewardship.....	4
Program Operations Managers Can Improve Privacy Culture	4
Recommendations.....	12
Management Comments and OIG Analysis	12

Figures

Figure 1: ICE’s Purposes for Personally Identifiable Information	3
Figure 2: Pillars of Privacy Stewardship	3
Figure 3: ICE Reported Privacy and Security Incidents.....	7
Figure 4: Training Recommendations by Survey Respondents.....	9
Figure 5: Privacy Integration in Information-Sharing Access Agreements.....	11

Appendixes

Appendix A: Purpose, Scope, and Methodology.....	14
Appendix B: Management Comments to the Draft Report	15
Appendix C: Legislation, Memorandums, Directives, and Guidance.....	17
Appendix D: The <i>Fair Information Practice Principles</i>	18
Appendix E: Component-Level Privacy Office Designation and Duties	19
Appendix F: Selected Systems: PII Collected, Privacy Impact Assessments, System of Records Notices, and Information Sharing.....	20
Appendix G: ICE Culture of Privacy Survey	21
Appendix H: Major Contributors to This Report	22
Appendix I: Report Distribution	23

Abbreviations

BMIS Web	Bond Management Information System Web Version
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
FIPPs	<i>Fair Information Practice Principles</i>
FISMA	<i>Federal Information Security Management Act</i>
ICE	Immigration and Customs Enforcement
NCVIS	National Child Victim Identification System
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
PIA	Privacy Impact Assessment
SEVIS I	Student and Exchange Visitor Information System
SORN	System of Records Notice

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We performed an audit of Immigration and Customs Enforcement's privacy stewardship. Our audit objectives were to determine whether Immigration and Customs Enforcement's plans and activities instill a culture of privacy and whether it complies with federal privacy laws and regulations. Appendix A provides our purpose, scope, and methodology.

Immigration and Customs Enforcement has made progress instilling a culture of privacy. Specifically, it demonstrated an organizational commitment to privacy compliance by appointing a privacy officer and establishing the Immigration and Customs Enforcement Privacy Office. The Privacy Office provides guidance to program and system managers who collect personally identifiable information on meeting requirements for notice, incident reporting, and privacy impact assessments. In addition, the Privacy Office has established processes for initial and annual privacy training and for addressing access, complaints, and redress for individuals.

We are making three recommendations to the Assistant Secretary to strengthen Immigration and Customs Enforcement's privacy stewardship. Immigration and Customs Enforcement can improve its culture of privacy by (1) developing and implementing privacy procedures and job-related privacy training to safeguard personally identifiable information in program operations, (2) establishing penalties for violations that correspond with Department of Homeland Security privacy rules of conduct, and (3) establishing a standardized process that includes Immigration and Customs Enforcement Privacy Office review and approval of information-sharing access agreements that involve personally identifiable information.

Background

The *Privacy Act of 1974*, as amended, imposes requirements on agencies whenever they collect, use, or disseminate personally identifiable information (PII) in a system of records. 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. The Privacy Act grants to U.S. citizens and legal permanent residents, access and amendment rights with limited judicial review.

A mixed system is any system of records that collects, maintains, or disseminates PII about U.S. persons and non-U.S. persons. For mixed systems, *DHS Memorandum 2007-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, requires the Department of Homeland Security (DHS) to extend a variety of Privacy Act protections to all persons (including aliens).¹

Immigration and Customs Enforcement (ICE) is the largest DHS investigative agency. ICE is responsible for enforcing immigration laws and investigating people, money, and materials that support terrorist and criminal activities. Almost 18,000 employees in more than 400 offices around the world interact daily with the public or collect, use, and disseminate PII about the public.

Figure 1 shows purposes for PII collection by three of ICE's major operations and for the maintenance of this PII in eight mixed systems that we reviewed. In 2008, Detention and Removal Operations, with support from the Office of the Chief Financial Officer, processed nearly 80,000 bonds and removed almost 246,000 illegal aliens. ICE collects PII from more than 1 million students, visitors, and sponsors for law enforcement and immigration control. ICE agents use databases with more than 364,000 PII records on child victimization, money laundering, and gang activity.

ICE's Purposes for Personally Identifiable Information
<p>IMMIGRATION BONDS FOR DETAINEES Office of the Chief Financial Officer systems Bond Management Information System Web Version (BMIS Web) and Electronic Bonds (eBONDS)</p>
<ul style="list-style-type: none">▪ Records and maintains financial information on immigration bonds for aliens involved in removal proceedings▪ Verifies alien eligibility for bond release; processes and tracks the life cycle of bonds

¹ *DHS Memorandum 2007-01* does not create a right of judicial review for non-U.S. persons.

ICE's Purposes for Personally Identifiable Information
STUDENT IMMIGRATION ENFORCEMENT Office of Investigation Division 2 systems Student & Exchange Visitor Information System (SEVIS I) and SEVIS II
<ul style="list-style-type: none"> ▪ Maintains information on F, M, and J Visa users, their dependents, and associated schools and sponsors
GLOBAL CRIMINAL INVESTIGATIONS Office of Investigation Division 6 systems Data Analysis & Research for Trade Transparency System (DARTTS) and DARTTS Enterprise, National Child Victim Identification System (NCVIS), ICEGangs
<ul style="list-style-type: none"> ▪ Analyzes trade and financial data for money laundering or other import-export crimes ▪ Combats exploitation of children, child pornography, and child sex tourism ▪ Maintains information on gang members and associates and gang-related activity

Figure 1. ICE's Purposes for Personally Identifiable Information

Source: ICE Privacy Impact Assessments and System of Records Notices.

DHS components are responsible for complying with federal privacy laws and requirements. *Privacy Policy Guidance Memorandum 2008-01* establishes the *Fair Information Practice Principles* (FIPPs) as the DHS privacy policy framework. The FIPPs are a set of principles that govern the collection, handling, and maintenance of PII. Appendix C lists federal requirements and guidance related to ICE's privacy stewardship.

As illustrated in figure 2, the level of organizational commitment to privacy accountability drives the expectations for privacy stewardship at executive management, program operations management, and employee levels. Effective privacy stewardship includes (1) ongoing privacy risk assessment and mitigation; (2) standardized procedures that implement the FIPPs and other requirements; and (3) established privacy conduct, training, and safeguards in program operations.



Figure 2. Pillars of Privacy Stewardship

Source: Adapted from DHS Privacy Office, DHS Privacy Framework.

A component's culture of privacy results from how well its executive management, program operation managers, and employees understand, implement, and enforce its privacy commitment in their respective roles. 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.

Results of Audit

ICE Has Made Progress in Privacy Stewardship

ICE demonstrated its commitment to privacy stewardship by designating a privacy officer and establishing a privacy office. The ICE Privacy Office provides privacy guidance, training, and assistance in assessing risks to PII. In addition, ICE has implemented processes for privacy notice, access, complaints, correction, and redress for individuals.

Privacy Office

In April 2008, ICE established the ICE Privacy Office by designating a privacy officer who is responsible for providing support and guidance for integrating privacy requirements into program operations. The ICE Privacy Office consists of five staff members. The ICE Privacy Office reports to the ICE Assistant Secretary's Chief of Staff. See appendix E for the duties that component privacy officers are required to perform. The ICE Privacy Office performs the following activities:

- Serves as point of contact with the DHS Privacy Office.
- Communicates privacy initiatives through its network site, which links to individual privacy laws, regulations, and policies, as well as to the DHS Privacy Office's public website.
- Provides additional guidance on privacy integration at points in the information technology system life cycle, instructions for reporting a privacy incident, and privacy tips on its network site. In a survey that we conducted, almost 75% of respondents who collect, handle, view, or maintain PII reported that they look for privacy guidance on the ICE Privacy Office network site.²
- Monitors privacy compliance when responding to privacy questions and assists managers in drafting privacy compliance documentation.
- Manages ICE's privacy incident responsibilities as defined in the DHS Privacy Office's *Privacy Incident Handling Guidance* and notifies the DHS Privacy Office of PII incidents.

² In November 2009, the OIG emailed to the ICE workforce a survey on its culture of privacy. The survey solicited opinions on how ICE employees could improve their understanding of privacy. See appendix G for the methodology and details of the survey.

Initial and Annual Privacy Training

In compliance with Office of Management and Budget (OMB) M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, the ICE Privacy Office provides initial privacy training for new employees and annual refresher privacy training for current employees. As of October 2009, the ICE Privacy Office began participating in all biweekly new employee orientation briefings to emphasize the importance of privacy as a core value at DHS. In October 2009, 34% of ICE's survey respondents reported that they received privacy training when they were hired.

ICE complies with the annual training requirement by requiring that employees take the Information Assurance and Awareness Training, which includes a module on safeguarding PII. The ICE Office of Training and Development monitors and retains employee training records, which show that 93% of employees (16,526 of 17,795) completed the training in FY 2008. In October 2009, the ICE Privacy Office implemented a Culture of Privacy Awareness course. Topics include penalties for noncompliance with key privacy laws, obligations to report privacy incidents, and a test on applying privacy procedures in various scenarios.

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.³ *DHS Handbook 4300A* requires a risk assessment every 3 years or whenever there are significant changes to the system. See appendix F for details regarding the PIAs on the systems that we reviewed.

The ICE Privacy Office is making progress in obtaining approvals of its PIAs. In November 2009, the DHS Office of the Chief Information Officer reported that 51% (19 of 37) of ICE's operational PII systems have approved PIAs.⁴ In March 2010, ICE had 66% approved PIAs and in May, the ICE Privacy Office achieved a 72% completion rate.

³ A Privacy Impact Assessment is the result of an analysis of how PII is collected, used, disseminated, and maintained, and represents how ICE has incorporated privacy concerns throughout the development, design, and deployment of a program, system, technology, or rulemaking.

⁴ The DHS Office of the Chief Information Officer developed an application, Trusted Agent FISMA, as an enterprise compliance management tool that tracks data related to DHS components' security status and privacy impact assessments, as well as plans of action and milestones to correct deficiencies.

According to the DHS Privacy Office *Privacy Impact Assessments Official Guidance*, every system that collects PII should have a retention schedule describing how long the information will be retained. Retention schedules ensure that components retain PII for as long as necessary to fulfill the specified purpose of collection. In compliance with OMB Circular A-130, ICE program operations managers work with the Records Management Branch to submit a records retention schedule to the National Archives and Records Administration for approval and registration. As of November 2009, 89% (33 of 37) of ICE's PII systems are in the approval process.

Processes for Privacy Notice, Access, Complaints, Correction, and Redress for Individuals

ICE provides notice to individuals regarding the component's collection, use, dissemination, and maintenance of PII in three specific ways:

- ICE provides Privacy Act statements for individuals from whom PII is collected on forms and websites.
- The ICE Privacy Office's public website shows its mission statement, contact information, and privacy notice.
- The ICE Privacy Office provides assistance and guidance to program operations managers regarding the development and approval process for Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).⁵ ICE has 30 PIAs and 13 SORNs that are approved by the DHS Privacy Office and are available on its public website.

The ICE Privacy Office has processes to receive privacy complaints and requests for access, correction, and redress from individuals. Through its Privacy Office Tracking System, the ICE Privacy Office tracks and resolves such complaints. Information on ICE and other component privacy complaints is available on the DHS Privacy Office public website.

Program Operations Managers Can Improve Privacy Culture

As stewards, program operations managers are in a unique position to provide leadership and instill a culture of privacy by promoting the importance of protecting privacy to their employees. ICE program

⁵ The System of Records Notice explains to the public how PII owners can exercise their rights granted through the Privacy Act.

operations managers can improve the overall privacy culture by instilling an internal discipline of applying privacy safeguards in four key areas:

- Minimizing privacy incidents by developing operational procedures that integrate privacy protections into daily work activities;
- Providing job-specific privacy training and oversight;
- Enforcing DHS privacy rules of conduct; and
- Applying privacy policies to PII sharing with external agencies.

Program Operations Managers Are Instrumental in Minimizing Privacy Incidents

DHS has privacy rules of conduct that can apply to different jobs and operations. However, about 45% of ICE’s survey respondents did not respond or responded incorrectly to questions regarding proper privacy procedures as set forth in the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information*.

As indicated in figure 3, 72% (114 of 159) of all incidents were reported under one of two categories: alteration/compromise of information or misuse.⁶ Twenty-eight percent (45 of 159) of incidents related to unauthorized access to ICE resources or other incidents.

DHS Categories of ICE Incidents	2-yr Period Incidents	Privacy Incidents			Security Incidents		
		2008	2009	% change	2008	2009	% change
Alteration/Compromise of Information	86	28	29	4%	19	10	- 47%
Misuse	28	2	0	- 100%	19	7	- 63%
Unauthorized Access	5	1	1	0%	2	1	- 50%
Other	40	0	0	0%	8	32	300%
Totals	159	31	30	- 3%	48	50	4%

Figure 3. ICE Reported Privacy and Security Incidents (2008 and 2009)
Source: DHS Security Operations Center.

We analyzed each of the 61 privacy incidents reported for 2008 (31) and 2009 (30). Sixty-two percent (38 of 61) of privacy incidents over the 2-year period involved the use of information systems. The remaining 38% (23 of 61) resulted from loss or theft of PII in laptops, mobile media devices, smart phones, hard drives, and paper files under the responsibility of ICE employees or contractors. We determined that 97% (59 of 61) of the incidents

⁶ The DHS Privacy Office’s *Privacy Incident Handling Guidance* defines privacy incidents as unauthorized access or potential access to PII in usable form, whether physical or electronic.

occurred because employees or contractors did not follow DHS privacy rules of conduct. The remaining 3% (2 of 61) occurred because of improper implementation of system security controls.

Managers and employees who we interviewed or surveyed told us that they have existing protocols and standards that provide privacy protection. For example, detention standards include the security of detainee records handled by nearly 8,000 Detention and Removal Operations personnel across 24 field offices, 161 subfield offices, and 22 detention service centers. Yet, we identified numerous instances during the 2-year period (2008 and 2009) of employees failing to protect PII. For example:

- An ICE employee sent an unencrypted email containing PII to a personal email account.
- Through inventory control, ICE discovered that a former ICE agent had lost his laptop, on which unencrypted investigative PII and physical security vulnerability reports were accessible.
- An unencrypted personal thumb drive containing PII of Student Exchange Visitor Program exchange visitors was stolen from an ICE employee attending a conference in India.
- Although an exiting ICE employee was debriefed, he left with a CD with the PII of 6,000 ICE agents. This incident was discovered by the new employing agency that found the PII and contacted ICE.
- Detainee records have been shared with individuals who did not have a need for this information, but these privacy incidents were not reported.
- In a hotel, ICE agents lost paper PII of individuals under investigation.
- Hundreds of paper PII records pertaining to ICE employees were left in a laptop case that was sold at a government auction.

The inability of employees to apply DHS rules of privacy conduct to their jobs and operations places PII at risk. As supervisors, program operations managers can promote an understanding of the importance of privacy and help employees apply privacy rules to the work setting. An additional layer of security results when job-specific privacy procedures are embedded as shared attitudes, values, goals, and practices in the workplace. When employees are reminded of privacy implications and proper procedures for handling PII, they may avoid causing privacy incidents. Furthermore, by establishing an internal discipline for proper

handling of PII, program operations managers can instill and improve the overall culture of privacy.

ICE Needs Job-Related Privacy Training to Comply With Requirements

OMB M-07-16 requires job-specific privacy training and recommends that agencies augment training through creative methods, job-specific communications, and advanced training to promote and improve the employees’ understanding of their privacy responsibilities. Yet, fewer than 7% of survey respondents reported receiving specialized or advanced privacy training. Although the ICE Privacy Office provides initial and annual privacy training, ICE employees need a better understanding of how to integrate privacy protections into their daily work.

Figure 4 shows that 87% (273 of 315) of survey respondents indicated that the available training and communication of privacy requirements are too general to be effective for their program-level application. Respondents recommended the following improvements: (1) more frequent, innovative, job-specific training (46%), (2) in-person training (30%), and (3) improved communication of privacy requirements (11%). Only 13% (42 of 315) of respondents—most of who do not handle PII—indicated that the present privacy training is acceptable.

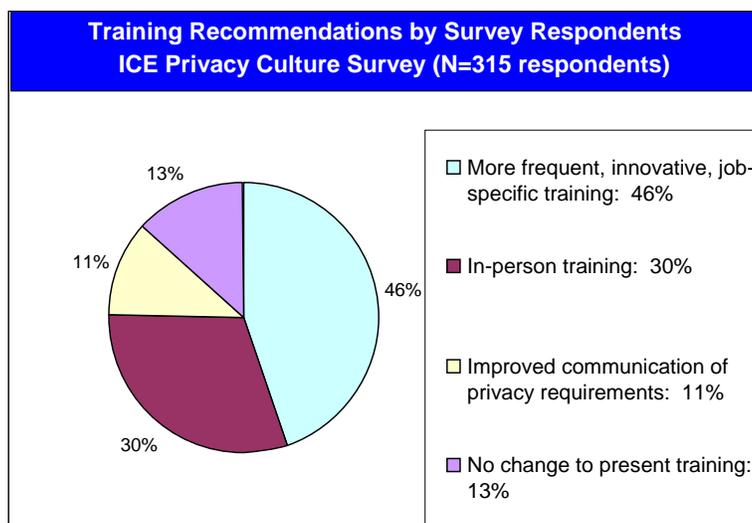


Figure 4. Training Recommendations by Survey Respondents

Source: OIG Analysis, ICE Culture of Privacy Survey.

ICE relies on computer-based privacy training to expand its reach to almost 18,000 employees located in more than 400 offices worldwide. Therefore, in-person training is limited. The ICE Privacy Office is improving communications by meeting with

groups regarding privacy compliance. The FIPPs for privacy accountability require managers and supervisors to provide training that integrates privacy safeguards into the daily work of employees and contactors who handle PII. However, program operations managers, who can provide in-person privacy training, coaching, and reminders, have not had the resources for customizing operational procedures to include privacy protections.

Forty-six percent of survey respondents requested more frequent and innovative job-specific privacy training. Program operations managers who we interviewed have not had the administrative support for implementing innovative or job-related privacy training. If they do not have the appropriate type and level of training and reinforcement of privacy protections, employees and system users who collect, use, or maintain PII may be careless or may not understand their responsibilities. The public's PII may be exposed to unnecessary risks.

ICE Needs Adequate Enforcement of Penalties for Privacy Rules of Conduct

ICE managers do not have specific penalties for privacy violations that correspond with the DHS privacy rules of conduct according to the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information*. The need for specificity in the existing ICE Table of Offenses and Penalties causes inadequate enforcement of penalties for privacy violations. In 2008 and 2009, managers enforced penalties for 31% (19 of 61) of all reported privacy violations.

In October 2008, the ICE Privacy Office recommended inclusion of privacy conduct into the existing rules of security behavior and changes to the ICE Table of Offenses and Penalties as an efficient way to enforce employees' privacy obligations. At present, the agency and union reviews have not been completed.

Information-Sharing Access Agreements Do Not Adequately Address Privacy

ICE has information-sharing access agreements for exchanging information when there is a need to share such information with external agencies to carry out national security, immigration, law

enforcement, or intelligence functions.⁷ DHS Information Sharing Coordinating Council developed a standardized process for the creation and approval of information-sharing access agreements that includes a privacy review. For example, the *DHS Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy* requires that these agreements describe how the FIPPs have been implemented in the information-sharing environment.⁸ See appendix D for the eight FIPPs principles.

None of the 11 information-sharing access agreements that ICE provided to us implemented all of the eight FIPPs. Figure 5 illustrates the incompleteness and inconsistencies of these agreements, through which ICE shares large volumes of financial data and the public’s PII. See appendix F for details on the systems’ information sharing.

System Names	BMIS Web	SEVIS I	DARTTS	ICEGangs
Fair Information Practice Principles	Did Information-Sharing Access Agreements Address the FIPPs?			
Security	Yes	Yes	Yes	Yes
Use Limitation	Yes	No	Yes	Yes
Purpose Specification	No	Yes	Yes	No
Accountability and Auditing (incl. Training)	No	No	Yes	No
Transparency	No	No	Yes	No
Data Minimization	No	No	No	Yes
Data Quality and Integrity	No	No	No	Yes
Individual Participation	No	No	N/A	N/A

Figure 5. Privacy Integration in Information-Sharing Access Agreements
 Source: 11 ICE information-sharing access agreements.

According to the DHS Information Sharing Access Agreements Methodology Guidebook, component program operations managers are responsible for working with their privacy representatives to draft new information-sharing access agreements and update legacy agreements. As ICE’s privacy representative, the ICE privacy officer is best situated to identify the privacy issues related to ICE’s mission and understand how best to implement DHS privacy policies.

Based on our review of nine agreements, ICE managers have not followed the Information Sharing Coordinating Council’s methodology or DHS privacy policies. There is no indication that

⁷ An information-sharing access agreement is any memorandum of understanding, memorandum of agreement, letter of understanding, letter of agreement, or any form of agreement that is used to facilitate the exchange of information between two or more parties.

⁸ The information-sharing environment is an approach that facilitates the sharing of terrorism information.

the ICE Privacy Office or a privacy representative was involved in the development of these agreements. In addition, there are omissions in addressing privacy considerations when sharing information. Consistently implementing the FIPPs through these agreements would ensure that sharing agencies have agreed to comply with protocols for handling PII, data quality needed for the specified use, reliability of data sources, data security, and minimizing data sharing to the amount necessary to meet the purpose of the agreement.

In addition, legacy agreements have not been updated to reflect current DHS guidance. Therefore, both legacy and newer agreements have omissions in addressing privacy considerations. Without a standardized process at the component-level to ensure that all PII information sharing has a privacy review prior to drafting agreements, mistakes, misunderstandings, data misuse, and incidents can occur.

Recommendations

We recommend that the Assistant Secretary of ICE:

Recommendation #1: Direct program operational managers to develop and implement privacy procedures and job-related privacy training to safeguard PII in program operations.

Recommendation #2: Establish penalties for violations that correspond with DHS privacy rules of conduct.

Recommendation #3: Establish a standardized process that includes the ICE Privacy Office for the review and approval of information-sharing access agreements that involve PII.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Secretary of ICE. We have included a copy of the comments in appendix B.

ICE concurred with our findings and recommendations. Concerning recommendation #1, ICE is taking steps to provide training on supervisory roles to support privacy awareness and compliance. We consider recommendation #1 open, pending our review of the finalized course documentation and training schedule by ICE.

ICE concurs with recommendation #2. ICE indicated it plans to adopt the DHS "PII Acknowledgement and Agreement" form that identifies penalties for violations of privacy rules of conduct. Also, ICE is considering amendments to the ICE Table of Offenses and Penalties. We consider recommendation #2 open, pending our review of ICE's adoption of the "PII Acknowledgement and Agreement" form and other actions.

ICE concurs with recommendation #3. According to ICE, it follows the DHS process for the review and approval of information sharing access agreements that involve PII. ICE also stated that the agreements reviewed by the OIG for the audit are older agreements drafted prior to the creation of the ISCC standards and prior to the existence of the ICE Privacy Office. As clarification, our review included both older agreements and agreements drafted after the establishment of the ISCC standards and ICE Privacy Office. We consider recommendation #3 open, pending our review of documentation that defines the process for engagement and the role of the ICE Privacy Office for component level review and approval of all ICE information sharing access agreements.

Appendix A

Purpose, Scope, and Methodology

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

We interviewed officials from the DHS Privacy Office and discussed its implementation of the DHS Privacy Framework and duties of component privacy officers. In addition to interviewing ICE's Privacy Officer and Chief Information Security Officer, we interviewed more than 70 program managers and information system security professionals at ICE headquarters and field sites. We emailed a survey to the ICE workforce to obtain their recommendations for improving their understanding of privacy and for an indication of their privacy knowledge. Four hundred and seventy of the 1,274 respondents offered written comments on the status, issues, suggestions, or challenges in ICE privacy stewardship. (See appendix G.)

We selected a sample of 8 systems from a total of 37 systems that handle personally identifiable information. For this sample, we reviewed technical information, system security documentation, architectures, financial justifications, privacy impact assessments, SORNs, application of the *Fair Information Practice Principles*, and ICE and program-level application of federal and DHS privacy laws and guidance.

Our analysis is based on direct observation, review of applicable documentation, and interviews. We conducted this performance audit between August 2009 and May 2010 in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Appendix B Management Comments to the Draft Report

Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536



U.S. Immigration
and Customs
Enforcement

June 10, 2010

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology Audits
Office of Inspector General

FROM: Martin N. Finkelstein 
Deputy Chief Financial Officer (Acting)
U.S. Immigration and Customs Enforcement

SUBJECT: Comments to OIG Draft Report "ICE Privacy Stewardship" dated May 2910

U.S. Immigration and Customs Enforcement (ICE) appreciates the opportunity to comment on the draft report. In response to OIG's recommendations for action by ICE:

Recommendation # 1: Direct program operational managers to develop and implement privacy procedures and job-related privacy training to safeguard PII in program operations.

Response # 1: ICE concurs. ICE has already implemented basic privacy training for all employees and created a training plan that will deliver through various means specialized privacy training and guidance to employees based on their assigned roles, duties and responsibilities. In addition, ICE will soon implement privacy training for ICE supervisors that will make them aware of their obligation as supervisors to develop and implement privacy protections in procedures and policies governing their program areas.

ICE requests this recommendation be considered resolved and closed.

Recommendation #2: Establish penalties for violations that correspond with DHS privacy rules of conduct.

Response # 2: ICE concurs. The DHS Privacy Office established privacy rules of conduct in its *Handbook for Safeguarding Sensitive Personally Identifiable Information*. Regarding consequences, the DHS Privacy Office in consultation with the Chief Human Capital Office (CHCO) and Office of General Counsel (OGC) developed a "PII Acknowledgement and Agreement" form that identifies penalties for violations of the rules. This form is currently under a final review by CHCO, and OGC and will be implemented as part of the Culture of Privacy Awareness training course on DHScovery. In addition, ICE is considering amendments to the ICE Table of Offenses and Penalties that will clarify existing definitions of violations to correspond with the *Handbook for Safeguarding Sensitive Personally Identifiable Information*.

Appendix B Management Comments to the Draft Report

Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536



U.S. Immigration
and Customs
Enforcement

ICE requests this recommendation be considered resolved and open.

Recommendation #3: Establish a standardized process that includes the ICE Privacy Office for the review and approval of information-sharing access agreements that involve PII.

Response # 3: ICE concurs. DHS has a standardized process that already exists and is being implemented by ICE that requires the participation of the Privacy Office in the review and approval of ICE information sharing access agreements (ISAAs) that involve PII. The DHS Information Sharing Coordination Council (ISCC) *Information Sharing and Access Agreement Methodology Guidebook* (February 2008) requires the participation of a privacy representative in the ISAA drafting process (*see* p.6). The ISAA Questionnaire, which is intended to collect the information needed to form an ISAA, also requires the participation of the privacy representative in answering certain questions (*see* p.6, Appendix A). The agreements reviewed by the OIG for this audit are older agreements drafted prior to the creation of the ISCC standards and prior to the existence of the ICE Privacy Office.

ICE requests this recommendation be considered resolved and closed.

Should you have questions or concerns, please contact Michael Moy, OIG Portfolio Manager, at (202) 732-6263, or by e-mail at Michael.Moy@dhs.gov.

Appendix C

Legislation, Memorandums, Directives, and Guidance Related to ICE 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>

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>

The Freedom of Information Act, 5 U.S.C. § 552, Public Law 104-231, 110 Stat. 3048 (1996).
http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

OMB Circular A-130: Management of Federal Information Resources, November 28, 2000.
<http://www.whitehouse.gov/omb/assets/omb/circulars/a130/a130trans4.pdf>

OMB M-09-29: FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (August 20, 2009). http://www.whitehouse.gov/omb/assets/memoranda_fy2009/m09-29.pdf

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

DHS Memorandum: Designation of Component Privacy Officers (June 5, 2009). (No external link available)

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

Privacy and Civil Liberties Policy Guidance Memorandum 2009-01: The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy (June 5, 2009).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf

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

Privacy 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: 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: Privacy Incident Handling Guidance (September 10, 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 4300A: Sensitive Systems Handbook Version 7.1 (November 13, 2009). (No External Link Available)

Appendix D

The Fair Information Practice Principles

The DHS Privacy Office, *Privacy Policy Guidance Memorandum Number 2008-01*, December 29, 2008, adopted the *Fair Information Practice Principles* as its privacy policy framework for application by DHS programs and activities.

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

Appendix E
Component-Level Privacy Office Designation and Duties

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

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

Appendix F
Selected Systems: PII Collected, Privacy Impact Assessments, System of Records
Notices, and Information Sharing

System Name and PII Collected	Privacy Impact Assessment	System of Records Notice	Information Sharing
Operational Systems			
Data Analysis and Research for Trade Transparency System (DARTTS) collects contact information about U.S. and foreign importers, exporters, brokers, and consignees; identification numbers for importers, exporters, and brokers; and U.S. financial data that includes Social Security and tax identification numbers, bank account information, and passport information.	Data Analysis and Research for Trade Transparency System (DARTTS) October 20, 2008, Updated April 26, 2010	Trade Transparency Analysis and Research (TTAR) October 31, 2008	DARTTS shares information with law enforcement entities for investigatory purposes and with other federal, state, local, and foreign agencies. DARTTS shares its reports on trade anomalies with other DHS components for law enforcement purposes. DARTTS uses trade data provided by federal agencies, foreign governments, and financial data collected by Customs and Border Protection and the Department of Treasury Financial Crimes Enforcement Network.
Bond Management Information System Web Version (BMIS Web) collects information about bonded aliens, individuals posting the bond (obligors), surety companies or bonding agencies, and bond information such as amount, bond number, or date posted.	Bond Management Information System Web Version (BMIS Web) August 25, 2008, Updated November 20, 2009	Bonds Management Information System (BMIS) September 11, 2008	BMIS Web shares information, as needed, with the Internal Revenue Service and the Department of Justice regarding interest paid to obligors, collections on monies owed on a bond, and investigations of a surety bonding agent/agency of financial stability, licensing, or business practices.
Electronic Bonds (eBONDS) will collect information such as an alien's name, A-number, bondable status, and detention location; the bond requester's name and address; surety agent's name, username, and password; and surety company's name, address, email address, and phone number.	Electronic BONDS July 14, 2009	Bonds Management Information System (BMIS) September 11, 2008	eBONDS shares information with the surety agents that have requested bond for an alien. eBONDS provides alien information to notify surety agents that an alien is eligible for a bond and to facilitate the creation of the bond documentation package by the surety agent.
Student and Exchange Visitor Information System (SEVIS I) collects information about certified schools, designated sponsors, foreign students or exchange visitors, and their dependents during their stays in the United States.	Student and Exchange Visitor Information System February 5, 2005 (out of date)	Student and Exchange Visitor Information System March 22, 2005 (out of date)	SEVIS I shares information with certified schools, designated sponsors, and exchange visitors. SEVIS I exchanges data with DHS components and other federal agencies such as the Department of State and Department of Justice.
National Child Victim Identification System (NCVIS) is a repository of 164,000 child victim images. Agents use the images as an aid for international law enforcement activities against child exploitation crimes.	National Child Victim Identification System (NCVIS) August 21, 2009	NCVIS is not a system of records. A SORN is not required.	NCVIS shares information with state, local, and tribal government and federal law enforcement agencies when these agencies submit an unconfirmed image to the ICE Cyber Crime Center to request a match. The images are never shared with non-law enforcement entities.
ICEGangs collects information about gang members or associates directly from individuals during normal law enforcement investigative activities such as arrests, field interviews with an informant, or by reviewing evidence.	ICEGangs Database January 15, 2009	Intelligence Records System (IIRS) December 9, 2008, 73 FR 74735	ICEGangs is a database that shares information regarding gangs, gang members, and gang associates when there is a need for this information by state, local, and tribal government and federal law enforcement agencies, as well as DHS components such as Customs and Border Protection.
Non-Operational Systems			
Student and Exchange Visitor Information System (SEVIS II) will collect the same information as SEVIS I.	Student Exchange Visitor Information System II December 4, 2009	Student and Exchange Visitor Information System II January 5, 2010	Not available
Data Analysis and Research for Trade Transparency System (DARTTS) Enterprise will collect the same information as DARTTS.	See DARTTS	See DARTTS	Not available

Source: The DHS Privacy Office has ICE Privacy Impact Assessments and System of Records Notices at http://www.dhs.gov/about/structure/editorial_0338.shtm (accessed January 21, 2010).

Appendix G ICE Culture of Privacy Survey

OIG developed a privacy questionnaire with involvement of the ICE Privacy Office. The purpose of the survey was to obtain employees' recommendations for improvements in understanding privacy.

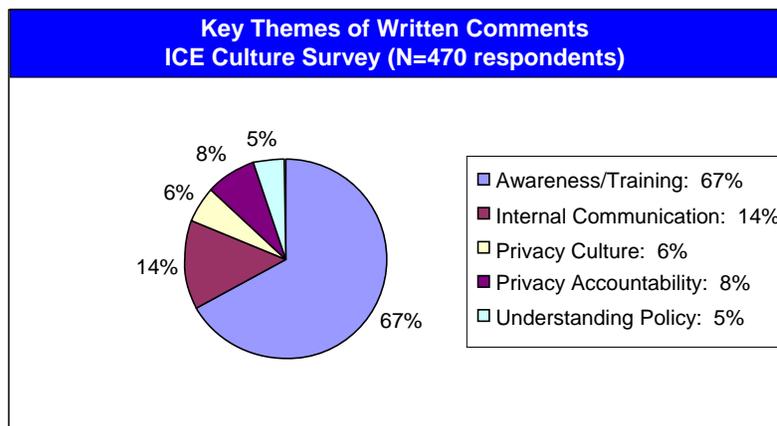
In October 2009, the OIG emailed the ICE workforce a link to a secure site to complete an online privacy questionnaire. Participation was voluntary, confidential, and accessible only by the OIG. The results of the survey provided insights into areas in which improvements are needed. The following figure provides the levels of job responsibility, location, and lengths of services for respondents who either completed the survey or provided selected responses.

Demographics Of Participants Of ICE Culture Survey		
Level of Job Responsibility	Location	Length of Service
Entry-level employees (15.9%) Mid- to high-level (nonmanager) employees (64.4%) Supervisors/managers (19.7%)	Headquarters (21.6%) Field offices (68.5%) Other (9.9%)	Less than 3 months (4.2%) 3–12 months (11.5%) 1–3 years (22.6%) More than 3 years (61.7%)

Source: OIG Analysis, ICE Culture of Privacy Survey.

Of the 1,274 respondents, 53.6% (683) completed the survey, 23.6% (300) provided selected responses, and 22.8% (291) initiated the survey but did not provide further response. The completed survey response rate was 3.8% (683 of 17,795).⁹

The following figure shows our grouping of 470 written comments by survey respondents. There are five key themes: privacy awareness and training (67%), internal privacy communications (14%), privacy accountability (8%), privacy culture (6%), and understanding policy (5%). The report provides a more detailed analysis regarding improvements in privacy awareness and training.



Source: OIG Analysis, ICE Culture of Privacy Survey.

⁹ Throughout the report, we used the FY 2008 training base population provided to us by the ICE Office of Training and Development.

Appendix H
Major Contributors to this Report

System Privacy Division

Marj Leaming, Director
Eun Suk Lee, Lead Privacy Auditor

Hung Huynh, Privacy Specialist
Cory Missimore, Privacy Specialist
Kevin Mullinix, Management and Program Assistant

Amanda Strickler, Referencer

Appendix I
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Policy
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
Assistant Secretary for Immigration and Customs Enforcement
DHS Privacy Office
ICE Audit Liaison Office
ICE Privacy Office

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.