Department of Homeland Security

Office of Inspector General

Radio Frequency Identification Security at USCIS Is Managed Effectively, But Can Be Strengthened

OIG-14-99

June 2014

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 5, 2014

MEMORANDUM FOR: Mark Schwartz
Chief Information Officer
United States Citizenship and Immigration Services

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Radio Frequency Identification Security at USCIS Is Managed Effectively, But Can Be Strengthened*

Attached for your information is our final report, *Radio Frequency Identification Security at USCIS Is Managed Effectively, But Can Be Strengthened*. We incorporated the formal comments from United States Citizenship and Immigration Services in the final report.

The report contains three recommendations aimed at improving the effectiveness of the radio frequency identification program. Your office concurred with all three recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Based on information provided in management's response to the draft report, we consider all three recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate congressional committees with oversight and

appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment

Table of Contents

Executive Summary 1

Background 2

Results of Audit 5

Infrastructure Established To Manage RFID Technology Effectively 5

Improvements Needed To Strengthen RFID Management 6

CPSTR Security Patches Were Not Deployed Timely 6
Recommendation 8
Management Comments and OIG Analysis 8

Assessments of ICPS Security Controls Were Not Performed Timely 8
Recommendation 9
Management Comments and OIG Analysis 9

Some ICPS Users Had Not Completed Annual Privacy Awareness Training ... 10
Recommendation 10
Management Comments and OIG Analysis 11

Appendixes

Appendix A: Objectives, Scope, and Methodology 12
Appendix B: Management Comments to the Draft Report 13
Appendix C: Major Contributors to This Report 15
Appendix D: Report Distribution 16

Abbreviations

CPSTR	Card Personalization System Technology Refreshment
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
ICPS	Integrated Card Production System
IT	information technology
NPS	National Production System

OIT	Office of Information Technology
PII	personally identifiable information
RFID	radio frequency identification
USCIS	United States Citizenship and Immigration Services
WHTI	Western Hemisphere Travel Initiative

Executive Summary

United States Citizenship and Immigration Services (USCIS) manages the permanent resident card program. Permanent resident cards, commonly known as green cards, provide identification for citizens of other countries who have been granted authorization to live and work in the United States on a permanent basis. The permanent resident cards currently produced by USCIS use radio frequency identification technology as both a security feature and means of expediting border crossings.

Radio frequency identification technology is a form of automatic identification and data capture technology that uses electric or magnetic fields at radio frequencies to transmit information. The use of radio frequency identification technology has introduced new security risks to agency systems. The flexibility and portability of radio frequency identification technology and devices increase the need for security. Without effective security controls, unauthorized users can obtain a compatible reader to read data stored on a card equipped with radio frequency identification technology; intercept and read data transmitted through the air; or access data stored in the system databases.

Our overall objective was to determine whether USCIS has effectively managed the implementation of radio frequency identification technology. We determined that USCIS has effectively managed the implementation of radio frequency identification technology by establishing an information technology infrastructure to secure personal information and implementing safeguards to minimize the risk of using radio frequency identification-enabled permanent resident cards. For example, USCIS has granted its card production system the authority to operate, evaluated privacy implications of using the system, and ensured that no personal data is transmitted by permanent resident cards. However, USCIS had not deployed timely security patches on the servers and workstations that support radio frequency identification processes, assessed annually the effectiveness of security controls implemented on the system that produces radio frequency identification cards, or ensured employees producing these cards receive the mandatory annual privacy awareness training.

We are making three recommendations to the USCIS Chief Information Officer. USCIS concurred with all recommendations and has begun to take actions to implement them. USCIS' responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

USCIS oversees lawful immigration to the United States. Its mission includes administering immigration and citizenship services, promoting awareness and understanding of citizenship, and ensuring the integrity of the Nation's immigration system. As part of its mission, USCIS manages the permanent resident card program. Figure 1 depicts a sample permanent resident card.

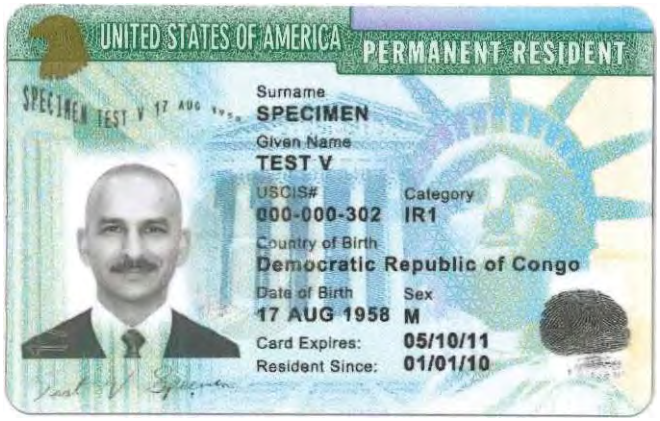

Figure 1. Permanent Resident Card

In response to the *Intelligence Reform and Terrorism Prevention Act*, the Departments of Homeland Security and State implemented the Western Hemisphere Travel Initiative (WHTI) on June 1, 2009. This initiative established document requirements for travel by land or sea into the U.S. from Canada, Mexico, the Caribbean, and Bermuda.[1] To comply with WHTI, travel documents must have radio frequency identification (RFID) capabilities for use at border crossings.

RFID technology is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. An RFID system can identify many types of objects to support a wide range of applications, such as asset management and access control. Each object requiring identification has a small device known as an RFID tag affixed to or embedded within it. The tag has a unique identifier and may hold additional information about the object. Devices known as RFID readers wirelessly communicate with the tags to identify the object and read or update additional information stored on the tag. A subsystem composed of common information technology (IT) components such as servers, databases, and workstations that can

[1] The *Intelligence Reform and Terrorism Prevention Act* called for implementation of a plan to require a passport or other authorized travel document deemed sufficient to denote identity and citizenship for all travel into the country, with the goal of expediting travel for those who frequently cross our borders.

benefit from typical IT security controls often supports this system of tags and readers. Figure 2 depicts the components of a typical RFID system.

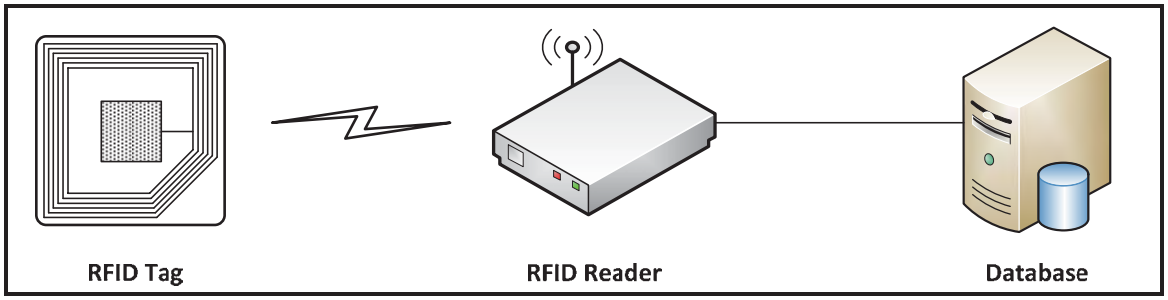

Figure 2. Components of an RFID System

Tags are categorized into four types based on the power source for communication and other functionality—passive, active, semi-active, and semi-passive. Tags need power to perform functions such as sending radio signals to a reader, storing and retrieving data, and performing other computations (e.g., those needed for security mechanisms). Passive tags, like those in permanent resident cards, use the electromagnetic energy they receive from a reader's transmission to reply to the reader and are typically less expensive, smaller, and lighter than active tags.

The use of RFID technology has introduced new security risks to agency systems. The flexibility and portability of RFID technology and devices increase the need for security. Without effective security controls, any compliant reader can read data on a tag; unauthorized devices can intercept and read data transmitted through the air; and unauthorized users can access data stored in the system databases.

USCIS began to issue RFID-enabled permanent resident cards in May 2010. Since then, USCIS has utilized the Integrated Card Production System (ICPS) to produce and issue more than 6.7 million RFID-enabled permanent resident cards. ICPS is composed of the following subsystems:

- ICPS Print Services – Converts applicant data to a form appropriate for card production and sends card production requests to the National Production System (NPS).

- NPS – Acts as a management system to centrally monitor and control card requests.

- NPS Web – Serves as an intranet for card production staff, adjudicators, and service center personnel to monitor system performance, set operating parameters, produce reports, and manage the central NPS application.

- Secure Mail Initiative – Allows USCIS customers to obtain the delivery status of secure identity documents through the USCIS National Customer Service Center.

- Card Personalization System Technology Refreshment (CPSTR) – Extracts the biographic and biometric data from NPS and returns production results to NPS after card production. USCIS erases all personal information from CPSTR within 72 hours of card production.

USCIS produces permanent resident cards at its Corbin Production Facility in Corbin, KY. Figure 3 depicts ICPS production equipment at the facility. We evaluated security controls implemented to secure the workstations that operate this equipment.

Figure 3. ICPS Equipment at the Corbin Production Facility

Results of Audit

Infrastructure Established To Manage RFID Technology Effectively

USCIS has effectively managed the implementation of RFID technology. For example, the component has established an information technology infrastructure to secure personal information and implemented safeguards to minimize the risk of using RFID-enabled permanent resident cards. The IT infrastructure incorporates the security elements required by the Department of Homeland Security (DHS), the *Federal Information Security Management Act* (FISMA), and the Office of Management and Budget. Specifically, USCIS has taken the following actions to secure ICPS and the personal information stored on and processed by the system:

- Adopted DHS security policies and procedures for RFID usage and adheres to applicable DHS requirements.

- Authorized ICPS to operate for a period of three years in July 2011, as required by FISMA.

- Developed and implemented a comprehensive system security plan for ICPS, as required by FISMA. In addition, USCIS maintains an up-to-date plan of action and milestones for known IT security weaknesses. We did not identify any deficiencies in the system security plan or plan of action and milestones.

- Ensured that ICPS users have received security awareness training, and users with significant security responsibilities have received specialized training.

- Performed a privacy threshold analysis for ICPS that the DHS Privacy Office approved February 2014. According to the analysis, USCIS addressed the privacy implications of using ICPS in a privacy impact assessment covering several USCIS systems associated with processing immigration applications and petitions.

- Implemented procedures at its Corbin Production Facility to secure permanent resident cards throughout the production process by restricting physical access to cards and recording the movement of card stock from receipt at the facility through shipment to card holders.

- Minimized the data stored on RFID tags in permanent resident cards to include only a unique identification number, and deletes CPSTR database records containing personal information within three days of card production.

- Protected against the cloning of RFID tags by procuring RFID-enabled cards with a unique tag identifier.

To evaluate the security of RFID tags and determine whether personally identifiable information is stored on permanent resident cards, we used a commercially available RFID tag reader to access the information stored on sample cards provided by USCIS. Through our testing we were able to read the tags embedded in permanent resident cards at a range of 25 feet. However, since the strength of the tag reader can affect the distance at which an individual can read the RFID tag in a permanent resident card, an attacker can use a more powerful reader to increase this range. To mitigate this threat, USCIS provides a protective sleeve with each permanent resident card to shield the RFID tag. When placed within one of these sleeves, we were unable to read the RFID tag of a permanent resident card at any range.

We were able to extract the RFID tag information from the sample permanent resident cards; however, no personally identifiable information (PII) or sensitive information was stored on the RFID tags. The only information stored on the RFID tag is a unique identifier that can be used to retrieve additional information stored in a Customs and Border Protection database. In the event that a malicious user may obtain this unique identifier to generate a duplicate signal at border crossings, the threat can be minimized through visual inspection of travelers and permanent resident cards. As a result, exposure of the unique identifier contained in the RFID tag poses minimal risk.

Improvements Needed To Strengthen RFID Management

While USCIS has taken actions to secure personal information and implement safeguards to minimize the risk of using RFID-enabled permanent resident cards, we identified deficiencies with technical security controls, annual assessments, and privacy training. Specifically, USCIS had not deployed security patches on the CPSTR servers and workstations timely, assessed the effectiveness of security controls implemented on ICPS annually, or ensured ICPS users complete the required privacy awareness training annually.

CPSTR Security Patches Were Not Deployed Timely

USCIS has not applied the required security patches to CPSTR timely.[2] Additionally, USCIS was unable to determine the patches installed on CPSTR. As

[2] Security patches are software updates that help prevent exploitation of applications and operating systems by mitigating vulnerabilities.

part of our audit, we conducted vulnerability assessments on CPSTR servers and workstations. Our assessments identified the following vulnerabilities:

- Java patches dating back to 2008 were missing on 27 of the 31 Windows workstations reviewed.[3] Failure to patch applications such as Java could allow an attacker to exploit vulnerabilities to gain access the system.

- A security patch that prevents an attacker from remotely executing arbitrary code was missing on both of the CPSTR Windows servers. Arbitrary code execution may allow an attacker to gain full access to the affected servers along with the data they process and store.

- Twenty-two critical patch updates were missing on servers running an Oracle database. Oracle critical patch updates are a collection of security fixes for Oracle products released quarterly.

DHS 4300A Sensitive Systems Handbook requires components to mitigate system vulnerabilities by promptly installing security and software patches. The DHS Security Operations Center publishes Information Security Vulnerability Management messages that dictate the timeframe in which components must install these patches. Additionally, *National Institute of Standards and Technology Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations* requires that agencies promptly install security-relevant software updates.

USCIS uses centralized and automated patch deployment software to identify and install updates to the workstations and servers that connect to its network. However, a firewall that segregates CPSTR from the rest of the USCIS network prevents Office of Information Technology (OIT) personnel from determining if they had installed the patches on the CPSTR network. To mitigate this limitation, OIT mails a disc containing patches to personnel at the Corbin Production Facility quarterly. Personnel at this facility then install the provided patches to each CPSTR server or workstation individually. However, since OIT cannot accurately determine if they had installed the patches, many patches are not added to the disc and installed as needed. According to OIT, it plans to fully integrate CPSTR with the USCIS network by the second quarter of fiscal year 2015, which will allow OIT to automatically deploy security patches directly to CPSTR.

[3] Java is a computer programming language used to develop applications.

CPSTR servers and workstations remain vulnerable until OIT identifies and applies the missing critical and high-risk patches. Failure to deploy software patches timely may expose USCIS to unnecessary risks such as the theft of PII. Ensuring CPSTR servers and workstations are up-to-date with security patches minimizes this risk, and protects CPSTR computers and the sensitive information they process and store.

Recommendation

We recommend that the Chief Information Officer:

Recommendation #1:

Expedite CPSTR's integration into the USCIS network to facilitate the timely identification and deployment of security patches to protect the sensitive information processed and stored by the system.

Management Comments and OIG Analysis

USCIS concurred with recommendation 1. The integration of CPSTR into the USCIS network is already in progress and OIT plans to complete this process by August 2014.

We agree that the steps USCIS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until USCIS provides supporting documentation that all planned corrective actions are completed.

Assessments of ICPS Security Controls Were Not Performed Timely

USCIS did not perform annual assessments to evaluate the effectiveness of security controls implemented on the systems comprising ICPS. OIT instead conducted monthly vulnerability scans to identify missing patches. However, OIT cannot assess the effectiveness of certain security controls through vulnerability scanning, such as contingency plan testing, restriction of physical access to systems, or incident reporting. Further, our review of the results of OIT's September 2013 vulnerability scan of CPSTR revealed that OIT scanned less than 10 percent of CPSTR computers. In addition, the OIT scans failed to identify many of the vulnerabilities that we identified during our evaluation.

FISMA requires that agencies perform periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, at least annually. This must include testing of management, operational, and technical controls.

According to OIT personnel, they no longer perform annual assessments of security controls because the DHS Office of Chief Information Officer has not issued requirements for performing the assessments since fiscal year 2011. Further, OIT personnel said that their monthly vulnerability scanning adheres to the guidance they have received from DHS indicating that there should be more focus on continuous monitoring for technical controls. However, until continuous monitoring is fully implemented, annual monitoring is necessary to ensure the periodic evaluation of all controls.

Further, while continuous monitoring efforts, such as vulnerability scans, can help to evaluate a sample of technical security controls, annual assessments provide additional evaluation of management and operational controls. Annual evaluations also serve to inform the authorizing official of changes that may affect the security of the system. Without results from annual assessments, OIT may not adequately inform management of the operating status of all types of security controls.

Recommendation

We recommend that the Chief Information Officer:

Recommendation #2:

Perform the required assessments periodically to evaluate the effectiveness of management, operational, and technical security controls implemented on ICPS and document the assessment results.

Management Comments and OIG Analysis

USCIS concurred with recommendation 2. As part of the ICPS reauthorization effort, USCIS recently completed a security control assessment to evaluate the effectiveness of the implemented management, operational, and technical security controls. By September 2014, USCIS plans to incorporate ICPS into the USCIS Ongoing Authorization program which will result in the assessment of security controls on a continual basis.

We agree that the steps USCIS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until USCIS provides supporting documentation that all planned corrective actions are completed.

Some ICPS Users Had Not Completed Annual Privacy Awareness Training

Some ICPS users had not completed the mandatory annual privacy awareness training. Of the 615 users with active ICPS accounts, 12 did not complete the training within the required timeframe. While this training is required of all DHS employees, it is of particular importance to those with access to ICPS as PII is stored in this system and used to produce permanent resident cards. We determined that some ICPS users had not completed privacy awareness training within the past year because management has not enforced the training requirement.

The Office of Management and Budget and DHS require that employees complete privacy and awareness training before permitting their access to agency information and information systems. After initial training, employees must complete online privacy refresher training annually.

Safeguarding and preventing inadvertent exposure of PII stored in and processed by the RFID system is essential to protect the privacy of applicants and ensure USCIS retains public trust. Through its permanent resident card program, USCIS users of ICPS have access to personal information of millions of permanent residents in the United States. Better enforcement of the requirement to complete privacy awareness training annually will help ensure this information is secure.

Recommendation

We recommend that the Chief Information Officer:

Recommendation #3:

Implement procedures to ensure and verify that ICPS users receive the required privacy training annually.

Management Comments and OIG Analysis

USCIS concurred with recommendation 3. USCIS' Office of Privacy has determined which Federal and contractor ICPS users have not completed the required annual privacy awareness training, and is actively communicating with these ICPS users and leadership to ensure the required training is completed by the end of May 2014. In addition, the Office of Privacy will continue to track and monitor ICPS users' completion of this annual course through monthly reports to USCIS leadership.

We agree that the steps USCIS is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until USCIS provides supporting documentation that all planned corrective actions are completed.

Appendix A
Objectives, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of our audit was to determine whether USCIS has effectively managed the implementation of RFID technology. Specifically, we determined whether USCIS has (1) developed proper policies and procedures to ensure the confidentiality, availability, and integrity of data on RFID tags, readers, and databases; (2) implemented effective security controls on its RFID devices to protect the data collected, processed, and generated; and (3) developed effective policies and procedures to protect the PII collected by and stored on the RFID system. Also, we determined whether USCIS systems using RFID technology were in compliance with FISMA requirements.

Our audit focused on requirements specified in the *DHS Sensitive Systems Handbook 4300A*, *United States Government Configuration Baseline*, and FISMA. We interviewed selected personnel and management officials from the Office of Information Technology, Office of Intake and Document Production, and DHS Office of Privacy. We performed fieldwork at USCIS offices in Washington, DC, and the Corbin Production Facility in Corbin, KY. We reviewed DHS policies and procedures for using RFID equipment, securing servers and workstations, completing IT security and privacy training, and reporting privacy incidents. In addition, we performed vulnerability and configuration scans using AppDetective and Nessus on 33 CPSTR servers and workstations at the Corbin Production Facility.

We conducted this performance audit between November 2013 and February 2014 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

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

Memorandum

MAY – 8 2014

TO: Richard Harsche
Acting Assistant Inspector General, Office of Information Technology Audits

FROM: Lori Scialabba
Acting Director

SUBJECT: U.S. Citizenship and Immigration Services Response to the Draft Report *"Radio Frequency Identification Security at USCIS is Managed Effectively, But Can Be Strengthened" For Official Use Only (OIG-13-165-ITA-USCIS)*

Thank you for the opportunity to review and comment on the subject Office of the Inspector General (OIG) draft report. In addition to this response, U.S. Citizenship and Immigration Services (USCIS) has separately provided technical and sensitivity comments related to the subject draft report.

The draft report positively notes USCIS's implementation of safeguards and establishment of an information technology infrastructure to secure personal information and minimize risk with radio frequency identification technology. The report further identifies measures USCIS can take to enhance the radio frequency identification program's overall effectiveness. Specifically, the OIG recommends that USCIS's Chief Information Officer take the following steps:

Recommendation 1: Expedite Card Personalization System Technology Refreshment (CPSTR) integration into the USCIS network to facilitate the timely identification and deployment of security patches to protect the sensitive information processed and stored by the system.

Response: USCIS concurs with this recommendation. The integration of CPSTR into the USCIS network is already in progress and the Office of Information Technology is scheduled to complete this process by August 2014.

Recommendation 2: Perform the required assessments periodically to evaluate the effectiveness of management, operational, and technical security controls implemented on Integrated Card Production System (ICPS) and document the assessment results.

Response: USCIS concurs with this recommendation. As part of the ICPS reauthorization effort, USCIS recently completed a security control assessment to evaluate the effectiveness of the implemented management, operational and technical security controls. By September 2014, ICPS will be adopted in the USCIS Ongoing Authorization program and the security controls will be assessed on a continual basis.

www.uscis.gov

Recommendation 3: Implement procedures to ensure and verify that ICPS users receive the required privacy training annually.

Response: USCIS concurs with this recommendation. USCIS's Office of Privacy has determined which federal and contractor ICPS users have not completed the required annual Privacy Awareness training, and is actively communicating with these ICPS users and leadership to ensure the required training is completed by the end of May 2014. In addition, the Office of Privacy will continue to track and monitor ICPS users' completion of this annual course through monthly reports to USCIS leadership.

Appendix C
Major Contributors to This Report

Chiu-Tong Tsang, Director
Mike Horton, IT Officer
Bridget Glazier, Lead IT Auditor
David Bunning, IT Specialist
Sheldon Liggins, IT Auditor
Anthony Nicholson, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
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, USCIS
DHS Component Liaison
Chief Privacy Officer
Chief Information Officer, USCIS
Chief Privacy Officer, USCIS
Chief, Office of Intake and Document Production, USCIS
Chief Information Security Officer, USCIS
Audit Liaison Team Lead, USCIS

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

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

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

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