Privacy Impact Assessment
for the

USCIS Investigations Division Case Management System (IDCMS)

DHS/USCIS/PIA-053

September 5, 2014

Contact Point
Donald K. Hawkins
Privacy Officer
US Citizenship and Immigration Services
(202) 272-8030

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Citizenship and Immigration Services (USCIS) Office of Security and Integrity (OSI) developed the Investigations Division Case Management System (IDCMS), an electronic case management system, to manage information relating to investigations of alleged USCIS employee and contractor criminal or administrative violations. USCIS is conducting this Privacy Impact Assessment (PIA) to assess the privacy risks associated with the collection, use, and dissemination of personally identifiable information (PII) contained in IDCMS.

Overview

In March 2007, the United States Citizenship and Immigration Services (USCIS) Director announced the creation of the Office of Security and Integrity (OSI) to enhance existing USCIS functions that focus on management integrity, individual integrity, and securing USCIS employees, facilities, information, and operations. One of OSI's functions is to conduct investigations of allegations of misconduct, corruption, and fraud involving USCIS employees and contractors. The OSI Investigations Division (INV) works with the Department of Homeland Security (DHS) Office of the Inspector General (OIG) to conduct investigations of alleged misconduct, corruption, and fraud involving any USCIS employee or contractor (employee).[1] INV is not involved in all OIG cases involving USCIS employees. For example, if an individual directs a complaint to OIG, INV would not be aware of it unless OIG brings INV into the investigation. INV uses the Investigations Division Case Management System (IDCMS) as both a tracking database for the USCIS employee misconduct cases handled by OIG of which INV is aware, as well as a case management system for cases investigated by INV.

Types of Employee Misconduct

Examples of alleged employee misconduct that INV or OIG may investigate include:[2]

- Fraud, corruption, bribery, and embezzlement;
- Theft or misuse of funds and theft of government property;
- Perjury;
- Physical assault;
- Unauthorized release of classified information;
- Drug use or possession;

[1] For the purposes of this PIA, all USCIS personnel, including federal employees or contractors, are considered employees.
[2] INV may only investigate noncriminal allegations of misconduct, corruption, and fraud involving a USCIS employee and which is not subject to investigation by OIG. *See* Homeland Security Act of 2002 § 453(a)(1), 6 U.S.C. § 273(a)(1).

- Unauthorized use of sensitive official government databases;
- Misuse of official position for private gain;
- Misuse of a government vehicle or property;
- Failure to properly account for government funds;
- Unauthorized use or misuse of a government purchase or travel card;
- Falsification of travel documents;
- Falsification of employment application documents;
- Misconduct by an employee at the General Schedule-15 level or higher;[3] or
- Arrest of an employee by law enforcement personnel.

Reporting Allegations of Employee Misconduct

Employees or members of the public who are victims of or witnesses to an act of employee misconduct may submit a complaint to INV or OIG.[4] DHS Management Directive 0810.1 specifies certain types of misconduct that DHS components must refer to OIG.[5] When a DHS component receives an allegation of misconduct that falls within one of the specified types of misconduct, the component must submit the allegation to OIG for review. OIG then determines if OIG or the respective DHS component has jurisdiction over the case. Appendix A of this PIA includes the list of allegations that require referral to OIG.

If an individual submits an allegation of misconduct directly to INV, INV enters the allegation into IDCMS and assigns the complaint a case number. If the allegation falls within the categories of misconduct identified in Appendix A, INV forwards the allegation to OIG through secure email for review and investigative determination. INV similarly processes allegations received from other federal, state, and local law enforcement agencies. The OIG either accepts the case and investigates the incident, or declines and returns the case to INV to handle as appropriate. USCIS creates a record in IDCMS even if USCIS sends the case to OIG to officially record receipt of the allegation and to begin the documentary chain of custody or audit trail.

[3] The General Schedule classification and pay system covers the majority of civilian Federal employees in professional, technical, administrative, and clerical positions. The General Schedule (GS) has 15 grades—GS-1 (lowest) to GS-15 (highest). Agencies establish (classify) the grade of each job based on the level of difficulty, responsibility, and qualifications required.
[4] For more information on how to report allegations of employee misconduct to the OIG, please visit http://www.oig.dhs.gov/.
[5] *See* DHS MD 0810.1, *available at* http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.

Information Collected as part of the Investigation

INV evaluates noncriminal allegations of misconduct, corruption, and fraud when the allegation involves a USCIS employee and is not subject to investigation by OIG. If INV determines an investigation is necessary, INV investigators collect information from and conduct interviews with: the individuals filing the complaint; the individuals alleged to have been involved in the violation; and individuals who have been identified as possibly relevant to, or who are contacted as part of, an OSI investigation.

INV may also review records (e.g., personnel, contract or grant, or financial files or records); collect forensic evidence; use surveillance and consensual monitoring; and use link analysis, databases, spreadsheets, and cyber forensics. INV also collects information from eyewitnesses, individuals who assisted the victim to cope with the incident, law enforcement agency personnel, and any other persons or entities with information pertinent to the matter under review. In addition, INV may collect and use publicly-available information from social media websites during an investigation.

Investigations Division Case Management System (IDCMS)

INV uses IDCMS to manage all information relating to INV investigations by recording disposition of allegations, tracking actions taken by USCIS management regarding misconduct, tracking cases that require legal action and referrals to the Department of Justice (DOJ) for prosecution, and creating and reporting statistical information about employee misconduct investigations.

Upon receiving allegations of misconduct, INV manually enters the complaint into IDCMS. The information from the complaint generally includes contact information of the individual submitting the claim and a description of the alleged incident.

INV then conducts its investigation and gathers relevant materials associated with the case. Throughout the investigation, INV updates IDCMS with electronic copies of part or all of the paper investigative files along with any electronic evidence.

Upon completion of either the OIG or INV investigation, INV transmits a Report of Investigation (ROI) to the appropriate USCIS manager and Human Capital and Training Labor and Employee Relations (LER) Program via secure email or mail for review and final disposition. If necessary, the USCIS manager consults with the LER servicing representative to determine whether the incident warrants further action. Regardless of the decision, the USCIS manager must provide a written response to the ROI, in the form of a *Management Report of Action*, no later than 90 days from the date of the ROI's cover memo to the office. The written response includes the administrative determination made by the office and indicates whether the report findings substantiated misconduct. If substantiated, the USCIS manager must also identify the action taken on the USCIS employee, which may include:

- Oral Admonishment, Counseling, or Reprimand;
- Alternate Dispute Resolution;
- Written Letter of Reprimand or Counseling;
- Suspension for a period of time;
- Restitution Made by the Employee;
- Demotion; or
- Termination, Resignation, or Retirement.

Once INV receives the final disposition response through the *Management Report of Action*, INV updates the case in IDCMS, reviews the case for quality assurance and case file completeness, and closes the case in IDCMS.

The information maintained in IDCMS is also used to generate reports as required by OIG and Congress. OSI creates a "Report on Internal Affairs Investigations" that responds to a requirement of section 109(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005.[6]

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Homeland Security Act of 2002 § 453(a)(1);[7] DHS Delegation Number: 0150.1; DHS Management Directive Number: 0810.1; and Memorandum of Understanding between the USCIS (formerly Bureau of Citizenship and Immigration Services) and the OIG authorize the collection of information by IDCMS.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Department of Homeland Security Internal Affairs SORN provides SORN coverage for IDCMS.[8]

[6] 8 U.S.C. § 1107.
[7] 6 U.S.C. § 273(a)(1).
[8] DHS/ALL-020 Internal Affairs System of Records, 79 FR 23361 (Apr. 28, 2014).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

IDCMS is a minor application under the Standard Lightweight Operational Environment-Application Development (SLOPE-AD) accreditation boundary. SLOPE-AD completed the security assessment and authorization documentation in August 2013 and was accepted into the Ongoing Authorization program by September 2013. The Ongoing Authorization requires SLOPE-AD, including IDCMS, to be reviewed on a monthly basis to maintain its security posture and maintain its ATO.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

NARA approved schedule N1-566-10-02 permitting USCIS to retain information related to USCIS employee misconduct. This schedule was approved on November 22, 2010. IDCMS retains all case records for 5 years. However, if OSI finds the case to be substantiated, IDCMS retains these case records for 10 years. IDCMS retains all cases with congressional interest for 50 years.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The collection of information for allegations of employee misconduct is not subject to the PRA. Based on the information that is collected and how the information is collected, the information contained in IDCMS is exempt from the PRA.[9]

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Through the collection methods described above, IDCMS may collect and maintain the following:

<u>Personally Identifiable Information (PII) related to the subject of the allegation:</u>

- First name;
- Middle name;

[9] *See* 5 CFR § 1320(h)(3).

- Last name;
- Last four digits of Social Security Number (SSN);
- Date of Birth;
- Alien File number, if applicable;
- OIG case number, if applicable;
- Significant Incident Report (SIR) number, if applicable;[10]
- Allegations of misconduct involving the subject;
- Email address;
- Office address;
- Office telephone number; and
- Employment information:
    - Title,
    - Grade, if applicable, and
    - Contract company, if applicable.

PII related to OSI investigators, complainants, witnesses, and victims:

- First name;
- Middle name;
- Last name;
- Title;
- Address;
- Phone number; and
- Email address.

[10] OSI also developed and implemented a web-based significant incident reporting capability for USCIS and providing reports on activities and trends to leadership and stakeholders. The SIR Number is a unique ID that is created in a separate system called GeoSpace. GeoSpace tracks any significant incidents that are reported to the USCIS Command Center. Some of these reports will involve incidents of employee misconduct. These SIR are encrypted and then sent to the Investigations Division Staff. The OSI INV Staff will then enter the SIR number in the Intake Record. A SIR is required when any event occurs in a USCIS office, domestic or international, that falls into one of the following major categories: Facilitated Apprehension; Office Closure, Evacuation, or Fire Alarm; Loss of Services or Utilities; Building/Physical Security Related Incidents; Information Spill/Mishandling; Lost, Stolen, or Damaged Government Property; and Employee/Contractor Events. *See* DHS/USCIS/PIA-047 – GeoSpace, *available at* www.dhs.gov/privacy for more information on this system.

If INV determines that an investigation is necessary, INV may collect additional information and enter it into IDCMS, including:

- Letters, memoranda, and other documents alleging criminal or administrative misconduct;
- Transcripts and documentation concerning requests and approval for consensual (telephone and non-telephone) monitoring;
- Reports from or to law enforcement entities;
- Prior criminal or non-criminal records of individuals as they relate to investigations;
- Subpoenas issued pursuant to OIG investigations and legal opinions, advice, and other legal documents provided by agency counsel;
- Reports of actions taken by management personnel regarding misconduct allegations and reports of legal actions, including actions resulting from violations of statutes referred to DOJ for prosecution;
- Records involving the disposition of investigations and resulting agency actions (e.g., criminal prosecutions, civil proceedings, administrative action);
- Medical record numbers; bank account numbers; health plan beneficiary numbers; certificate/license numbers; vehicle identifiers including license plates; marriage records;
- Government-issued mobile device identifiers and serial numbers;
- Uniform resource locators from Government-owned computers;
- Education records, biometric identifiers, photographs, and other unique identifying numbers or characteristics;
- Tracking information regarding the status of a specific pending OSI investigation;
- OSI ROIs;
- DHS ROIs and related documentation on USCIS employees from component investigative agencies; and
- Information migrated from INV's Case Management System 2.0 (CMS), the legacy OSI investigation information system.

In addition, IDCMS users may upload attachments into IDCMS case files. Attachments may include a scanned copy of the original allegation, memoranda from leadership, emails, or any other case-related material that would be stored in a paper file.

2.2 What are the sources of the information and how is the information collected for the project?

Individuals may submit an initial allegation of employee misconduct through the following methods:

- Employee Misconduct Form;[11]
- IDCMS Intake Email Address;
- Mail; and
- OSI Investigations Division Fax Line.

The following categories of individuals are sources of information contained in IDCMS:

- Complainants (e.g., employees and the public);
- Witnesses to the allegation;
- Victims of the allegation; and
- Federal, state, and local law enforcement agencies.

INV may collect additional information through various investigative techniques, including interviews with the complainants, witnesses, victims, and subjects of the complaints. INV may also collect information from appropriate record reviews (e.g., personnel files, financial records). However, investigative techniques and sources can greatly vary depending on the investigation.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

INV may use commercial databases and publicly available information, including information posted on social media websites, during an investigation to obtain background information; verify addresses, identities, and contact information; identify possible witnesses; and for other investigative purposes.

2.4 Discuss how accuracy of the data is ensured.

Each record has a unique file number to prevent duplication. INV verifies information contained in the complaint through the investigative process, which varies depending on the allegation and information at issue. INV uses investigative techniques to ensure that the

[11] The Employee Misconduct Form is located on the USCIS OSI Intranet page. Employees may submit the form online or print the form for mail or fax delivery. When submitted online, the information will be sent as an email to the IDCMS Intake email address.

information, evidence, and data collected is sufficiently reliable for making accurate and logical interpretations and judgments regarding the matter under investigation.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that IDCMS may maintain inaccurate data.

Mitigation: USCIS mitigates this risk by using system design features to minimize inaccurate or incorrect data being entered. For example, IDCMS uses drop down options for certain fields, such as Position and Title. This is a quality control step to minimize inaccurate data entry by users. Once a user initially enters a complaint into IDCMS, an INV investigator reviews the data, cross-references it to information gathered during the interviewing process, and may update any inaccurate data, as necessary.

Privacy Risk: There is a risk of collecting more information than needed to conduct an investigation.

Mitigation: INV collects information from various sources to have an accurate and complete picture of the incident. INV will only enter information into IDCMS if INV determines that the information is relevant to the investigation.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

When INV receives allegations of employee misconduct, OSI records the allegation in IDCMS. INV primarily uses the information collected to confirm the identity of the employee being accused of the criminal or administrative violation and to conduct any necessary investigation. The specific use of the information depends on the allegation under investigation. USCIS also uses data stored in IDCMS to generate reports that comply with congressional and DHS reporting requirements.

IDCMS employee misconduct case information is shared with OIG and USCIS leadership who have a need-to-know, including managers, Office of Chief Counsel, Office of Legislative Affairs, and the USCIS Director. These individuals do not have direct access to the system.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

No other components have assigned roles and responsibilities within IDCMS. However, USCIS may share IDCMS information with DHS Headquarters or other USCIS components for reporting, investigatory, evidentiary, or prosecutorial purposes, or for civil proceedings purposes. OSI shares information in IDCMS with other DHS components, including OIG, Transportation Security Administration, Customs and Border Protection, U.S. Coast Guard, Federal Emergency Management Agency, and U.S. Secret Service. USCIS works with other components on an as needed basis, depending on the particular circumstances of a case.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in IDCMS may be used for an unauthorized purpose.

Mitigation: USCIS mitigates this risk through the use of access controls and audit logs. Only USCIS personnel authorized by INV are granted access to the IDCMS. The INV Chief determines access to the system. IDCMS users are required to follow DHS policies to protect passwords and login information and only have access to case files needed to perform their assigned duties. In addition, IDCMS contains global audit log functionality that tracks every user movement throughout the system. The IDCMS Information Systems Security Officer is responsible for monitoring the audit log for unauthorized access and use. If an employee were to breach IDCMS policy, the audit log would identify the actions taken and the user responsible.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The Employee Misconduct Form instructions contain a Privacy Act Statement that notifies the individual about the authority to collect the information requested, purposes, routine uses, and consequences of providing or declining to provide information to USCIS. The publication of this PIA and the Internal Affairs SORN provide public notice of the collection, use, and maintenance of this information.[12]

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

USCIS employees have an official obligation to report suspected misconduct, although the reporting process allows for anonymity. Members of the public are not obligated to report allegations of misconduct; therefore, any information provided by the public is purely voluntary.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: An individual who is the subject of an allegation may be unaware that his or her information is being used for an investigation.

Mitigation: Notice to subjects of investigations may not be feasible at the point of collection since providing notice may result in disclosure of investigative techniques, procedures, and evidence. The publication of this PIA and Internal Affairs SORN provides transparency, but because of the nature of the investigative process, subjects of investigations may be unaware that their information is being used for an investigation until such time as they are interviewed. USCIS also provides notice during any interviews for complainants, witnesses, and victims of allegations.

[12] DHS/ALL-020 Internal Affairs System of Records, 79 FR 23361 (Apr. 28, 2014).

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

NARA approved the IDCMS record retention schedule, N1-566-10-02, on November 22, 2010. The record retention schedule states that IDCMS retains all unsubstantiated case records for 5 years and substantiated case records for 10 years. IDCMS retains all cases with Congressional interest for 50 years.

IDCMS retains records for unsubstantiated cases for 5 years in the event that INV receives a new complaint that is linked to an unsubstantiated closed case. This enables the investigator to have the greatest amount of historical information necessary to conduct the investigation on the new complaint. Substantiated records and those that have a congressional interest are retained for 10 and 50 years, respectively, for historical and reporting purposes.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that IDCMS may retain information for longer than is necessary for INV to conduct an investigation.

Mitigation: NARA signed the IDCMS retention schedule on November 22, 2010. The USCIS Records Officer and NARA carefully negotiated the schedule to ensure that the data is retained for the minimum time needed to conduct an investigation and respond to incoming congressional inquiries.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS in accordance with the routine uses found in the Internal Affairs SORN.[13]

The INV Chief may share employee misconduct case information with a congressional office in response to an inquiry. INV may also share information with federal, state, or local law

[13] *Id.*

enforcement agencies in support of criminal and administrative investigations. Lastly, INV may share information with witnesses as part of an investigation.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

USCIS's disclosure of information about employee misconduct is compatible with the Internal Affairs SORN because USCIS only externally shares IDCMS information within the bounds of an approved routine use. The DHS Internal Affairs SORN routine use B permits DHS to share information with a congressional office at the request of the individual to whom the record pertains, and routine use G permits DHS to share information with federal, state, or local law enforcement agencies.[14]

6.3 Does the project place limitations on re-dissemination?

Information is shared on a case-by-case basis and is transmitted in an ROI through a variety of methods including electronic communications through encrypted or password protected files attached to Outlook emails, briefings and interviews, and in writing through registered and tracked mail. ROIs include a cover sheet with the following language regarding re-dissemination: "This report contains sensitive official investigative material. It may not be loaned outside your agency and, except in connection with official agency action, no portion of the report may be copied or distributed without the knowledge and consent of the [USCIS] Office of Security and Integrity."

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

INV maintains a record of information sharing within the individual case file.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that IDCMS information may be used by external agencies for purposes that are not in accord with the stated purpose and use of the original collection.

Mitigation: USCIS is careful to share IDCMS data only with external agencies that have a need-to-know and for a purpose that is compatible with the Internal Affairs SORN. The Privacy Act Statement included on the Employee Misconduct Form notifies the individual that USCIS may provide information to other government agencies. As required by DHS procedures and policies, all current external sharing arrangements are consistent with the original purpose for which the information was collected.

[14] *Id.*

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

As noted in the Internal Affairs SORN,[15] the Secretary of Homeland Security exempted records within the Internal Affairs system of records from provisions of the Privacy Act, subject to the limitations set forth in 5 U.S.C. § 552a. An individual who is the subject of a record in IDCMS may access records that are not exempt from disclosure. USCIS determines whether the individual or another person may access a record at the time a request is received based on Freedom of Information Act (FOIA) exemptions or, if applicable, the Privacy Act exemptions found within the Internal Affairs SORN.

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to National Records Center, FOIA/PA Office, P.O. Box 648010, Lee's Summit, MO 64064-8010.

When seeking personal records from this system of records or any other USCIS system of records, the request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. Individuals requesting access to their records must first verify their identity by providing their full name, current address, and date and place of birth. The requestor must sign the request, and the signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, requestors may obtain forms for this purpose from the Director, Disclosure and FOIA, http://www.uscis.gov. In addition, requestors should: (1) provide an explanation of why they believe the Department would have information on him or her; (2) specify when he or she believe the records would have been created; and (3) if the requestor is seeking records pertaining to another living individual, include a statement from that individual certifying his or her agreement for the requestor to access his or her records. Without this information, USCIS will not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals have the opportunity to correct inaccurate or erroneous information during an interview with the INV investigator. Individuals can also submit requests to contest or amend

[15] *Id.*

information contained in IDCMS. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act to prevent harm to investigations.

Requests to contest or amend information contained in IDCMS should be submitted as discussed in Section 7.1. The requestor should clearly and concisely state the information being contested, the reason for contesting or amending it, and the proposed amendment. The requestor should also clearly mark the envelope, "Privacy Act Amendment Request." The record must be identified in the same manner as described for making a request for access.

7.3 How does the project notify individuals about the procedures for correcting their information?

The DHS Internal Affairs SORN[16] provides individuals with guidance regarding the procedures for correcting information and indicates that all or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to an investigation. This PIA also provides notice.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the right to redress may be limited by Privacy Act exemptions or limited avenues for seeking redress.

Mitigation: USCIS mitigates this risk by reviewing each request to determine whether USCIS may release the requested information and by releasing the information when there is not an exemption that prevents releasing the information.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

As part of the internal technical controls within IDCMS, case files are restricted to those persons with a need-to-know. Each record has an audit trail to track the modification and who made the changes (by person and date/time stamp). The IDCMS Administrator reviews the audit trail of all activities on the system on an as needed basis and when there is a change in the system to determine who made the change and whether the change was authorized and appropriate.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS mandates that system users to comply with Sensitive System Security guidelines

[16] *Id.*

and to complete mandatory annual Privacy and Computer Security Awareness training. They are then granted permission levels based upon their roles and responsibilities.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only personnel authorized by INV may access IDCMS. DHS requires these personnel to comply with Sensitive System Security guidelines and to complete mandatory annual Privacy and Computer Security Awareness training. USCIS uses role-based access controls to enforce a need-to-know policy to protect the confidentiality, availability, and integrity of personal data. USCIS also uses limited permission and information audit trails to mitigate the misuse of information. Additionally, each employee with access to IDCMS must first have a valid USCIS network account.

The INV Chief or his or her designee must approve any requests for personnel to become users of IDCMS. After the user successfully completes the required training, the user's account is activated, and he or she can begin using the system.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

USCIS has a formal MOU in place with the DHS OIG that was signed on April 17, 2003. This MOU formalizes the agreement OIG has with USCIS to investigate alleged cases of misconduct, or to refer cases back to USCIS.

Responsible Officials

Donald K. Hawkins
Privacy Officer
United States Citizenship and Immigration Services
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

Categories of Misconduct that must be referred to OIG[17]

- All allegations of criminal misconduct against a DHS employee;
- All allegations of misconduct against employees at the General Schedule 15 level or higher, or against DHS employees;
- All allegations of serious, noncriminal misconduct against a law enforcement officer. "Serious, noncriminal misconduct" is conduct that, if proved, would constitute perjury or material dishonesty, warrant suspension as discipline for a first offense, or result in loss of law enforcement authority. For purposes of this directive, a "law enforcement officer" is defined as any individual who is authorized to carry a weapon, make arrests, or conduct searches;
- All instances regarding discharge of a firearm that results in death or personal injury or otherwise warrants referral to the Civil Rights Criminal Division of the Department of Justice;
- All allegations of fraud by contractors, grantees or other individuals or entities receiving DHS funds or otherwise engaged in the operation of DHS programs or operations; and
- All allegations of visa fraud by DHS employees working in the visa issuance process.

In addition, the OIG will investigate allegations against individuals or entities that do not fit into the categories identified above if the allegations reflect systemic violations, such as abuses of civil rights, civil liberties, or racial and ethnic profiling, serious management problems within the department, or otherwise represent a serious danger to public health and safety.

[17] *See* DHS MD 0810.1, *available at* http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.