Privacy Impact Assessment Update
for the

Office of Inspector General Investigative Records System

September 24, 2009

Contact Point

Thomas Frost
Assistant Inspector General for Investigations
Office of Inspector General
Department of Homeland Security
(202) 254-4100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of Inspector General (OIG) Investigative Records System (IRS) includes both paper investigative files and the "Enforcement Data System" (EDS). EDS, although within IRS, is an electronic case management and tracking information system, which also generates management reports. OIG uses EDS to manage information relating to DHS OIG investigations of alleged criminal, civil, or administrative violations by DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS and to track resources used in investigative activities. This Privacy Impact Assessment (PIA) is an update to the PIA approved January 18, 2008. The update is necessary because EDS has been updated and is a new Web based system with enhanced security features and new data elements.

Introduction

Under the Inspector General Act of 1978, as amended, (5 U.S.C. App.), the DHS Inspector General (IG) is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DHS. The OIG promotes economy, efficiency, and effectiveness within the Department and prevents and detects fraud, waste, and abuse in its programs and operations. The OIG's Office of Investigations investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and Departmental programs and activities. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions. Additionally, the Office of Investigations provides oversight and monitors the investigative activity of DHS' various internal affairs offices.

IRS assists the OIG in receiving and processing allegations of violation of criminal, civil, and administrative laws and regulations relating to DHS employees, contractors, grantees, and other individuals and entities associated with DHS, and to document and track investigations undertaken by both OIG and component internal affairs offices. The system includes both paper investigative files and EDS. EDS, although within IRS, is an electronic case management and tracking information system that also generates management reports. EDS allows the OIG to manage information provided during the course of its investigations, and, in the process, to facilitate its management of investigations and investigative resources. Through EDS, which collects, processes, and stores personally identifiable information (PII), the OIG can create a record showing the disposition of allegations; track actions taken by management regarding misconduct; track legal actions taken following referrals to the U.S. Department of Justice for prosecution or civil action; provide a system for creating and reporting statistical information; and track OIG investigators' training as well as government property and other resources used in investigative activities.

Case-related documentation, including correspondence, memoranda of investigative activity, documentary evidence and photographs, witness statements, affidavits, investigative reports, and court documents are contained in IRS. Paper files and physical evidence are also included in IRS.

EDS and related paper investigative files are used for various purposes. For example, a typical transaction would involve reference to EDS to determine whether the subject of an investigation has been named in any other case currently being worked, or that has been closed, by the OIG. Another typical

transaction involves reviewing EDS for cases under a specific person's name in response to a Freedom of Information Act (FOIA) or Privacy Act request filed with the OIG by that person.

On October 6, 2005, DHS published a System of Records Notice (SORN) covering records collected under this system titled, DHS/OIG-002 Investigations Data Management System (October 6, 2005, 70 FR 58448). On January 30, 2008, DHS published a final rule for DHS/OIG-002 Investigations Data Management System (January 30, 2008, 73 FR 5421) exempting this system of records from certain provisions of the Privacy Act because it is a law enforcement system. DHS is updating both the SORN and final rule for DHS/OIG-002 Investigations Data Management System to include changes resulting from EDS. Changes in the SORN include a name change to IRS, additional routine uses, as well as changes to individuals and records covered by the system.

Reason for the PIA Update

The electronic case management portion of IRS has been redesigned to create a Web based system allowing an increased number of database users to accommodate an increasing investigative staff, an improved ability to search the database, and enhanced reporting capabilities.

EDS is a Web based system with:

- enhanced security features, including role based access and access control of individual records in the system;
- a more robust audit trail;
- new data elements including additional dates of case initiation and undercover operations;
- displays of mandatory contractor disclosures now required by the Federal Acquisition Regulation (FAR); and
- identification of privacy complaints for quarterly reporting required by section 803 of Public Law 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007.

Privacy Impact Analysis

In each of the sections below consider how the system has changed and what impact the changes have on the below Fair Information Practice Principles. In some cases there may be no changes and indicate as such.

The System and the Information Collected and Stored within the System

The type of PII collected and stored within EDS has not changed. The data fields and types of information contained in this system and identified in the PIA dated January 18, 2008, remain the same. However, a new source of information is now mandated by subpart 3.10 of the FAR, which requires government contractors to report credible evidence of violations of criminal law involving fraud, conflicts of interest, bribery, and gratuities and violations of the civil False Claims Act.

Privacy risks associated with this new source of PII in IRS include potentially inaccurate information because the PII is reported by a third party, such as a government contractor, and individuals

may not be aware that their PII is being collected by DHS OIG.

Mandatory contractor disclosures are handled like other hotline complaints, tips, or investigative leads. The disclosure is the start of the investigatory process. OIG investigators take diligent steps to ensure only relevant evidence is collected; that the investigation complies with all applicable law and policy; that it is carried out in an unbiased manner; that evidence is corroborated, and that sources are documented in sufficient detail to assess their reliability.

The mandatory disclosure rule was published in the Federal Register (November 12, 2008, 73 FR 67064) and received considerable attention in various public media as well as by relevant associations. The DHS OIG public Web site has a prominent link to pages describing the disclosure rule and provides a form for use in reporting under the rule. Ultimately, the subject is routinely interviewed as part of any investigation.

Uses of the System and the Information

The uses of the system have not changed. DHS OIG continues to use this system of records to fulfill its statutory mission under the Inspector General Act of 1978, as amended, to investigate allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, and Departmental programs and activities.

Retention

The National Archives and Records Administration (NARA) approved records schedule N1-563-07-05 for DHS OIG investigative records. Investigative case files that involve substantive information relating to national security or allegations against senior DHS officials, that attract national media or congressional attention, or that result in substantive changes in DHS policies or procedures are permanent records and are transferred to NARA 20 years after completion of the investigation and all actions based thereon. All other investigative case files are destroyed 20 years after completion of the investigation and all actions based thereon. Accountable property records, training and firearms qualification records, and management reports are destroyed when no longer needed for business purposes.

Internal Sharing and Disclosure

The inclusion of mandatory contractor disclosures could increase internal sharing because of the need to coordinate the investigation and any remedies with both the component contracting officer and counsel. Thus far, the number of contractor disclosures has been inconsequential.

Increased internal sharing could increase the risk of unauthorized access and disclosure. All DHS employees receive annual privacy training and DHS has appropriate policies in place for safeguarding PII, including specific guidance on marking and transmission.

External Sharing and Disclosure

Changes to IRS have not resulted in new external sharing and disclosure of PII. However, in proposing revisions to the SORN, OIG has proposed two new routine uses. One would allow notification

of a data breach in the system when disclosure is necessary to protect the interests of those whose data may have been improperly accessed or disclosed, or when necessary to prevent or minimize harm resulting from the breach. The second proposed routine use would allow disclosure from IRS to the news media and the public when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or in the event that it becomes necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system.

Any additional privacy risk resulting from the routine use for the media is mitigated by requiring approval of the Chief Privacy Officer and counsel prior to making any such disclosure.

Notice

Mandatory contractor disclosure is required by a new section of the FAR which was published in the Federal Register (November 12, 2008, 73 FR 67064). The collection is also described on the OIG's Web site. In addition, the proposed new routine uses will be published in the Federal Register with the revised SORN.

Individual Access, Redress, and Correction

Access, redress, and correction have not changed. When the revised SORN is published, a proposed rule continuing the exemption of IRS from these provisions of the Privacy Act will be published as well.

Technical Access and Security

EDS is a Web based system with enhanced security features, including role based access and access control of individual records in the system as well as a more robust audit trail. No added privacy risks were identified with these changes.

Technology

The automated part of IRS has been redesigned to create a Web based system allowing an increased number of database users to accommodate increasing investigative staff, an improved ability to search the database, and enhanced reporting capabilities. The production server is now separate from the database server and the database server has been upgraded. The software was changed from Cold Fusion to Microsoft .NET 2.0, resulting in the enhanced security features described above. No added privacy risks were identified. The changes allow layered security at the Web site, application, module, record, and page levels.

Responsible Official

Thomas Frost
Assistant Inspector General for Investigations
Office of Inspector General
Department of Homeland Security
(202) 254-4100

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security