Privacy Impact Assessment Update
for the

Office of Inspector General Enterprise Data System

DHS/OIG/PIA-001(b)

July 10, 2015

Contact Point

Yvonne Manino
Policy Specialist for Investigations
Office of Inspector General
Department of Homeland Security
(202) 254-4100

Reviewing Official

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

Abstract

The Department of Homeland Security (DHS) Office of Inspector General (OIG) maintains complaint and investigation related files on paper and in the electronic Enterprise Data System (EDS). EDS is the official OIG electronic case management system. OIG uses EDS to manage information relating to complaints and investigations of alleged criminal, civil, or administrative violations by DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS, and manage investigations born from those complaints to facilitate the tracking of resources used in investigative activities. This PIA update is necessary because (1) the PIA name has been changed from Investigative Records System (IRS) to Enterprise Data System; and (2) EDS has been modernized and now includes the capacity to retain biometric information for investigative purposes and OIG employee work performance history information.

Introduction

Under the *Inspector General Act of 1978*, as amended,[1] the Department of Homeland Security (DHS) Office of the Inspector General (OIG) is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DHS. OIG promotes economy, efficiency, and effectiveness within the Department and prevents and detects employee corruption, fraud, waste, and abuse in its programs and operations. OIG's Office of Investigations (OI) investigates allegations of criminal, civil, and administrative misconduct involving DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS and Departmental programs and activities. These investigations can result in criminal prosecutions, fines, civil monetary penalties, and administrative sanctions. Additionally, OI provides oversight and monitors the investigative activity of the DHS Components' various internal affairs offices.

The Enterprise Data System (EDS) is an electronic case management system that allows OIG to manage information provided during the course of adjudicating complaints and investigations and, in the process, to facilitate its management of investigations and investigative resources. Through EDS, which ingests, processes, and stores personally identifiable information (PII), OIG can create a record showing the disposition of allegations (i.e. complaints); audit actions taken by DHS management regarding employee misconduct; audit legal actions taken following referrals to the U.S. Department of Justice (DOJ) for criminal prosecution or civil action; provide a system for calculating and reporting statistical information; manage OIG investigators' training; and manage Government-issued investigative property and other resources used in investigative activities. EDS maintains complaint and investigation-related

[1] 5 U.S.C. App. 3.

documentation, including correspondence, memoranda of investigative activity, documentary evidence and photographs, witness statements, affidavits, investigative reports, OIG subpoenas, and court documents.

EDS and related paper complaint and investigative files are used for various purposes. For example, a typical transaction may involve referencing EDS to determine whether the alleged offender in an investigation has been named in other OIG complaints or investigations. OIG also uses EDS to review complaints and investigations under a specific person's name in response to a Freedom of Information Act (FOIA) or Privacy Act request filed with OIG by that person.

Reason for the PIA Update

This Privacy Impact Assessment (PIA) is an update to the DHS/OIG/PIA-001(a) Office of Inspector General Investigative Records System Update PIA, approved September 24, 2009. OIG is renaming this PIA to better reflect the name of the OIG information technology system, Enterprise Data System, as opposed to the more general Investigative Records System (IRS). Since the last PIA, EDS has been enhanced with a new capacity to store biometrics information. In addition, EDS processes and stores OIG employee performance appraisal information through its electronic Performance Appraisal System (ePAS) module.[2]

EDS maintains other information related to investigations: Time Tracking System (TTS), E-Subpoena, Special Agent Handbook (SAH), Investigations Forms and Exhibits, Organizational Property, Training, Law Enforcement Databases, Acting Manager, and Statistical Dashboard.

- Time Tracking System (TTS) – is designed for employees to record the number of hours spent on specific activities during the pay period. TTS allows for the tracking of hours spent on activities under (1) Direct Categories such as projects or cases, and (2) Indirect Categories such as travel or training.
- E-Subpoena – allows Special Agents to generate a subpoena request from an EDS case file.
- Special Agent Handbook (SAH) – provides instructions, guidance, and policy for OIG law enforcement personnel.
- Investigations Forms and Exhibits – allows access to forms and exhibits needed by Special Agents.

[2] Employee work performance records maintained within EDS are covered by OPM/GOVT-1 General Personnel Records (December 11, 2012, 77 FR 73694), OPM/GOVT-2 Employee Personnel File System Records (April 27, 2000, 65 FR 24732), and DHS/ALL-003 Department of Homeland Security General Training Records (November 25, 2008, 73 FR 71659).

- Organizational Property – captures inventory of Badges, Ballistic Vests, Firearms, Fleet, and Technical Equipment.
- Training – captures required annual training courses, overdue courses, courses completed, and the completion date.
- Law Enforcement Databases – displays a list of hyperlinks to other law enforcement databases.
- Acting Manager – allows Special Agents in Charge (SAC) or Assistant SACs to give permission to act on their behalf while away for an extended period of time.
- Statistical Dashboard – allows SACs and managers to view progress in their office(s).

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

EDS continues to maintain information about complainants, witnesses, and subjects as described in the January 18, 2008 and September 24, 2009 PIAs, including name; date of birth; mailing address; telephone number; Social Security number; email address; zip code; facsimile number; commercial data, for investigative purposes such as identifying potential witnesses, verifying addresses, tracing proceeds from illegal activities, and for other investigative purposes; and work-related information such as status of investigations, agencies involved, date opened and closed, type of investigation, allegations, and ultimate disposition of case. EDS will now also collect passport numbers, visa information, citizenship status, Alien Number (A-Number), and limited biometrics information. Passport numbers are collected during investigations when investigating agents locate Passports during the course of the investigation. Visa information, citizenship status, and alien information are collected during investigations when the complainant(s), witness(es), or subject(s) are not U.S. citizens.

As a law enforcement office, OIG OI secures fingerprints from offenders associated with administrative, civil, and criminal violations. Fingerprints are collected electronically from individuals suspected of committing an administrative, civil, or criminal violation under the DHS OIG's authority.[3] Elimination fingerprints are also collected to assist in exonerating persons accused of committing an offense. OIG collects fingerprints with a digital fingerprint scanner and sends them directly to DOJ's Joint Automated Booking System (JABS).[4] JABS is a conduit for sending standard booking data directly to the Federal Bureau of Investigation's (FBI) Next

[3] 5 U.S.C. App. 3.
[4] For more information on JABS, *see* DOJ Joint Automated Booking System PIA, *available at* http://www.justice.gov/sites/default/files/jmd/legacy/2014/06/27/jabs.pdf and JUSTICE/DOJ-005 Nationwide Joint Automated Booking System (JABS), 72 FR 3410 (Jan. 25, 2007).

Generation system. Fingerprints are not stored or shared with DHS's Automated Biometric Identification System (IDENT).

EDS is a complete management system that maintains information in addition to complaints and investigations. It also includes the Special Agent Handbook, the official policy for OI, official forms, timesheet, performance, and training and property records.

Privacy Risk: There is a risk of over-collection of sensitive PII associated with the collection of biometrics in EDS.

Mitigation: OIG mitigates this risk by limiting the purposes for which biometric information is collected. OIG only collects biometrics when necessary to assist in the investigation and conviction of individuals suspected of administrative, civil, and criminal violations.

Uses of the System and the Information

No change from the September 2009 PIA.

Retention

The National Archives and Records Administration (NARA) approved records schedule N1-563-07-05 continues to apply to DHS OIG investigative records. Complaint and investigative record 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 complaint and investigative record files are destroyed 20 years after completion of the investigation and all actions based thereon. Government issued accountable property records, training and firearms qualification records, and management reports are destroyed when no longer needed for business purposes.

For employee work performance history records, NARA approved records schedule N1-GRS-95-3 item 23a4, which requires the destruction of most summary performance appraisal records, including the performance appraisals and job elements and standards upon which they are based within four (4) years after the date of appraisal. Retention periods vary if the employee is part of the Senior Executive Service (N1-GRS-82-2 item 23b3), leaves the Department (N1-GRS-95-3 item 23a3a), or receives an appraisal of unacceptable performance (N1-GRS-93-3 item 23a1).

Internal Sharing and Disclosure

No change from the September 2009 PIA.

External Sharing and Disclosure

In addition to the data previously sent to DOJ, OIG will expand its sharing with DOJ to include biometrics.

Notice

DHS continues to provide notice to the public through this PIA and the Investigative Records System of Records notice (SORN).[5] DHS provides notice of the collection of OIG employee performance information through the Employee Personnel File System Records SORN.[6]

Individual Access, Redress, and Correction

No change from the September 2009 PIA.

Technical Access and Security

No change from the September 2009 PIA.

Technology

The automated part of EDS has been redesigned to create a Web-based system that increases the number of database users to accommodate increasing investigative staff, an improved ability to search the database, and enhanced reporting capabilities. The system modules specific to OI are used by approved OI staff. The ePAS and TTS modules in EDS are used by all OIG staff. The system also provides improved search capabilities including new filters and search (i.e., the ability to search for a complaint or investigation just using part of a record name instead of requiring the input of the entire record name). The production server is now separate from the database server and the database server has been upgraded. The software was changed from Microsoft.NET to Microsoft.NET 4.0 framework, resulting in the enhanced security features described above. The changes allow layered security at the Web site, application, module, record, and page levels.

Privacy Risk: By allowing users to search for a complaint or investigation by partial record name or partial complaint information, there is a risk that the search will not be narrowly tailored and may result in the retrieval of unrelated information.

Mitigation: This risk is partially mitigated. By policy, users are permitted to conduct searches of EDS for information related to official duties or for information that may assist in resolving or investigating complaints. OIG employees authorized to access EDS receive training on the appropriate use of the system. OIG Special Agents also receive specific direction through OIG directives and manuals that address the privacy interests in investigative materials. EDS

[5] DHS/OIG-002 Office of Inspector General (OIG) Investigative Records System of Records, 74 FR 55569 (Oct. 28, 2009).
[6] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35347 (June 19, 2006).

tracks user actions through an audit trail, which is regularly reviewed to ensure that individuals are using the system appropriately.

Responsible Official

Yvonne Manino
Policy Specialist
Office of Investigations
Office of Inspector General
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