Privacy Impact Assessment

for the

OIG Enforcement Data System (EDS)

DHS Reference No. DHS/OIG/PIA-001(c)

May 25, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) maintains complaint and investigation-related files within the Enforcement Data System (EDS). EDS is the official OIG electronic case management system for investigations. The OIG Office of Investigations, Office of Counsel, and the Whistleblower Protection Unit use 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. EDS also tracks resources used in investigative activities. This Privacy Impact Assessment (PIA) update documents several enhancements to the existing system.

Overview

Under the Inspector General Act of 1978, as amended,[1] DHS OIG is responsible for conducting and supervising independent and objective audits, inspections, and investigations of the programs and operations of DHS. DHS OIG promotes economy, efficiency, and effectiveness within DHS and prevents and detects employee corruption, fraud, waste, and abuse in its programs and operations.

EDS is a DHS-OIG Government off the Shelf (GOTS) application which is owned and operated by the Office of Investigations. EDS is the Office of Investigations' electronic case management system that allows for the managing of information provided during the process of adjudicating complaints and investigations and the coordination of investigative resources.

Through EDS, which ingests, processes, and stores personally identifiable information (PII), OIG can create a record showing the disposition of allegations (e.g., complaints), actions taken by DHS management regarding employee misconduct, and 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 property and other resources used in investigative activities. EDS maintains complaint and investigation-related 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 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 potentially responsive records related to a Freedom of Information Act (FOIA) or Privacy Act (PA) request.

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

Reason for the PIA Update

This Privacy Impact Assessment is an update to DHS/OIG/PIA-001(b) Office of Inspector General Enterprise Data System, approved July 10, 2015.[2] Since then, OIG has undertaken several enhancements to EDS. Such enhancements include the removal of the Time Tracking System (TTS) and electronic Performance Appraisal System (ePAS) modules, the removal of unnecessary stored procedures, the moving of document storage from file storage to database storage, and the use of entity frameworks. Additionally, EDS is now using Model View Controller (MVC).

The Time Tracking System was designed for employees to record the number of hours spent on specific activities during the pay period in the following categories: (1) Direct Categories such as projects or cases; and (2) Indirect Categories such as travel or training. This information is no longer tracked within EDS.

EDS previously processed and stored OIG employee performance appraisal information through the electronic Performance Appraisal System module. This module did not interact with EDS as anticipated and was subsequently removed from the EDS application.

Model View Controller provides a more secure environment for the system by using a less complex code that is delivered in the browser. This allows OIG to pinpoint and correct security vulnerabilities and lowers attack vectors. Model View Controller separates an application into three main, logical components: the model, the view, and the controller within the architecture of the site. This separation makes the code easier to maintain, reduces the risk of introducing bugs and security flaws, and provides a more robust authentication and authorization process, reducing response times and making it easier to manage permissions.

The use of entity frameworks has also made EDS more secure by (1) eliminating any possibility of Structured Query Language (SQL) injection attacks by using Language-Integrated Query-to-entity framework (LINQ-to-EF) and Structured Query Language query parameters; (2) performing basic sanitation of input; (3) making it easier to debug and test the stored procedures; and (4) making bug and security flaw resolution a smoother process.

Privacy Impact Analysis

Authorities and Other Requirements

The Inspector General Act of 1978, as amended, grants Inspectors General the authority to collect information necessary for the Office of Inspector General to perform audits, inspections, investigations, and legal analysis on programs and operations within the Department of Homeland

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT DATA SYSTEM, DHS/OIG/PIA-001(b), *available at* https://www.dhs.gov/privacy-documents-office-inspector-general-oig.

Security. Department of Homeland Security Management Directive System MD Number 0810.1 states the roles and responsibilities of the Heads of U.S. Department of Homeland Security Organizational Elements (OE), Department of Homeland Security employees, and the Office of Inspector General in collecting any files, records, reports, or other information that may be requested either orally or in writing. Specifically, the Directive assigns the OIG the responsibility to "receive and investigate complaints or information from employees, contractors and other individuals concerning the possible existence of criminal or other misconduct constituting a violation of law…."[3]

Characterization of the Information

EDS continues to maintain information about complainants, witnesses, and subjects, including name; date of birth; physical characteristics; race; 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. Moreover, EDS collects city, state, country of birth, country of citizenship, email address, pay grade and series information, past civil and criminal history, passport numbers, visa information, citizenship status, A-Number, photos, and biometric information, such as fingerprints. EDS further maintains complaint and investigation-related documentation, to include correspondence, memoranda of investigative activity, documentary evidence and photographs, witness statements, affidavits, investigative reports, OIG subpoenas, and court documents.

OIG also obtains information it maintains in EDS that relates to investigations during agent investigation interviews, and from the National Finance Center (NFC), OIG Hotline, and other law enforcement databases, such as the Joint Integrity Case Management System (JICMS).[4] The majority of collected information comes from records maintained by DHS Components. Information can also be obtained from other government agencies; government contractors and vendors; commercial sources, including third-party data aggregation firms; and publicly available sources, which may include public websites, news sources, open social media sites, and public geospatial data.

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY MANAGEMENT DIRECTIVE SYSTEM MD NUMBER 0810.1 (June 10, 2004*), available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_0810_1_the_office_of_inspector_general.pdf.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM, DHS/CBP/PIA-044 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

EDS no longer maintains records relating to the Time Tracking System, which captured the number of hours spent on specific activities during the pay period, or the electronic Performance Appraisal System module, which included OIG employee performance appraisal information.

Uses of the Information

EDS ingests, processes, and stores personally identifiable information (PII) to create a record in order to show the disposition of allegations (e.g., complaints); actions taken by DHS management regarding employee misconduct; legal actions taken following referrals to the U.S. Department of Justice (DOJ) for criminal prosecution or civil action; provides a system for calculating and reporting statistical information; manages OIG investigators' training; and manages government-issued property and other resources such as subpoenas and warrants used in investigative activities.

DHS OIG continues to use this information 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.

Notice

OIG continues to provide notice to the public through this Privacy Impact Assessment and the Investigative Records System of Records Notice (SORN).[5]

Data Retention by the Project

The National Archives and Records Administration (NARA) approved records schedule N1-563-07-05 continues to apply to DHS OIG investigative records within EDS. Complaint and investigative record files that involve substantive information relating to national security, refer to allegations against senior DHS officials, involve issues that attract national media or congressional attention, or result in substantive changes in DHS policies or procedures are permanent records and are transferred to the National Archives and Records Administration 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, or 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. 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).

[5] DHS/OIG-002 Office of Inspector General (OIG) Investigative Records System of Records, 86 FR 58292 (October 21, 2021).

Information Sharing

OIG may share investigative information with other law enforcement agencies with a verified need-to-know, U.S. Attorney's Office, and Congress on an as needed basis, pursuant to OIG's statutory and regulatory authorities and responsibilities. Information pertaining to an investigation may be provided to the corresponding law enforcement agency or internal affairs office who may also be conducting or following up on an investigation, as well as to prosecutors and defense attorneys. Information may also be shared with the trial court as part of the judicial process, as well as the Merit Systems Protection Board (MSPB) for administrative cases pertaining to employee misconduct. Any information shared outside of OIG is done so on a need-to-know basis, and only information that is required is shared. In some circumstances, certain data elements may be redacted prior to being referred and/or sent to the recipient.

Regarding sharing within OIG, those individuals deemed to have a need-to-know are provided user access to only the data they require. Such access is further controlled by using defined roles and setting restrictions for each case. Also, the ability to download data from EDS is restricted (e.g., to OIG Investigations personnel assigned to the case, OIG management), and downloads are only allowed if an articulable need exists, which is documented in the record.

Redress

Due to the nature of the information maintained in EDS, certain records may be exempt from requests for access by covered individuals, to the extent permitted by the Privacy Act and the DHS/OIG-002 System of Records Notice and associated Final Rule. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may still file a Privacy Act request to access their information. Depending on a review, analysis, and determination made by DHS OIG, those records may or may not be released.

Notwithstanding, all individuals seeking access to their records may submit a Freedom of Information Act (FOIA) request at https://www.oig.dhs.gov/foia. Requests can also be made by email, telephone, or mail:

OIG Office of Counsel
245 Murray Lane SW Mail Stop - 0305
Washington, D.C. 20528-0305
Phone: 202-981-6100
FOIA.OIG@OIG.DHS.GOV

OIG only maintains ownership of its own data and records. Therefore, OIG will refer FOIA and Privacy Act requestors seeking non-OIG data to the appropriate DHS Component. All requests must conform to the Privacy Act regulations set forth in federal regulations and are evaluated to ensure that the release of information is lawful, will not impede an investigation, and will not

reveal the existence of an investigation or investigative interest on the part of DHS or another agency.

Auditing and Accountability

EDS uses single sign-on via the OIG network for access to the system. Users are configured based on Role-Based Access Control (RBAC). Audit logs are configured to track any user login attempts and all activities while logged into EDS, including which cases a user accesses. EDS will also log any modification(s) made to the system, which user made the modification(s), and date and time of the modification(s). The OIG Office of Chief Information Officer, Information System Security Officer for EDS will review the logs monthly. Additionally, the OIG security team will perform the following audit techniques within EDS:

- Independent Verification and Validation (IV&V).
- Risk Assessments.
- Vulnerability Scanning.
- Third-party audits.

The OIG is also subject to inspection by the Committee on Inspector General Integrity and Efficiency (CIGIE). These inspections may review the OIG's use of EDS to determine if the system is being used in accordance with its stated purpose.

System administrators, cybersecurity professionals, and other individuals with specific roles and responsibilities are required to complete training specific to their job responsibilities. This includes ISSO training, application administrator training for each relevant application, incident response training, and other role-based courses.

Access to investigative information is determined by case assignment. A DHS OIG office supervisor, such as the Special Agent in Charge or Assistant Special Agent in Charge, will assign investigators to an investigation and notify the case agent of the assignments. Supervisors from affected external agencies will provide the DHS OIG office supervisor with a representative from those (external) agencies when a case involves a multi-agency investigation. Access to EDS is controlled, and therefore those designated representatives will receive a login once their need-to-know status is established. Such access will be further controlled by defined roles and restrictions. Investigators are considered to have a need-to-know for a case. All personnel authorized to access EDS receive training on the appropriate use of the system. All authorized users are notified during their onboarding to the system of the confidential nature of the data and prohibitions against misuse and improper disclosure.

Contact Official

Chad Steel
Special Agent in Charge
Office of Investigations
Office Inspector General
U.S. Department of Homeland Security

Responsible Official

Roy Jones
Chief, Information Law and Disclosure
Office of Inspector General
U.S. Department of Homeland Security

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717