Privacy Impact Assessment

for the

Joint-Threat Information Management System (J-TIMS)

DHS Reference No. DHS/ALL/PIA-084(d)

October 2, 2024

Homeland Security

Abstract

The Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO) is responsible for safeguarding the Department's people, information, and resources against constantly evolving security threats. The nature of OCSO's various specialized divisions has led to the development of the Joint Threat Information Management System (J-TIMS) as a centralized solution for managing intake and tracking the lifecycle of security-related events. OCSO is conducting this Privacy Impact Assessment (PIA) Update to include the integration with the Office of the Inspector General's (OIG) Law Enforcement Data Exchange (LEDX) to automate the allegation process within J-TIMS.

Overview

The primary mission of DHS is to prevent terrorism and enhance security, including the mitigation of risks and threats against the U.S. Government. Within DHS, OCSO's mission is to lead the collaborative security program to safeguard the Department's people, information, and resources so that the Department can secure the Homeland. As such, OCSO established J-TIMS to effectively and efficiently maintain the information necessary to fulfill that mission. Below are the J-TIMS modules that are part of a joint effort within the Threat Management Operations, Enterprise Security Operations and Support, and Headquarters Support Directorates to enable information sharing, referrals, and sending and receiving of leads to start and support cases. The primary goal of J-TIMS is to enable subject-specific information sharing across OCSO in real time to minimize redundant work and improve response timing and priority when required.

The initial J-TIMS launch included the following four modules that capture intake, security incidents, misconduct investigations, and cyber forensics cases:

- **Case Support Team Module** – The Case Support Team is primarily responsible for the intake of all reported incidents that meet approved guidelines. The Case Support Team triages Reported Events/incidents to determine the responsible office within which the incident falls. The Case Support Team subsequently creates a Reported Event within J-TIMS that is then referred to the appropriate DHS Component or OCSO Directorate.
- **Security Incident Reporting (SIR) Module** – The Security Incident Reporting Module provides a centralized tool for managing all security incidents. In addition, it streamlines the process of assigning Special Security Officers to conduct inquiries and make the final determination on the security incident.
- **Investigations and Operations Division (within the Threat Management Operations Directorate)) Module** – The Investigations and Operations Division conducts impartial, independent, and thorough criminal and administrative

investigations related to security incidents involving DHS personnel, information, or property. These investigations are predicated on allegations or information received about employees or contractors engaged in criminal or administrative misconduct. The Investigations and Operations Division Module maintains the capability to track allegations of criminal or administrative misconduct from receipt of the allegation until the Report of Investigation is completed. It provides a means to manage workflows, serves as a central repository of corrective actions, and aids in forming and generating both management and analytical reports.

- **Cyber Forensic Laboratory Module** – The Cyber Forensic Laboratory Module serves as a support function to the OCSO Investigations and Operations Division and other law enforcement and administrative investigative groups within DHS. The Cyber Forensic Laboratory Module conducts impartial cyber forensic examinations by using industry-standard best practices. This module is used as a solution to manage Cyber Forensic Laboratory cyber-service requests, cases, and case evidence.

J-TIMS has since expanded and created new modules to include employee allegations/misconduct, foreign activity inquiries, and employment suitability/security eligibility:

- **Office of Professional Responsibility (OPR) Module** – The Office of Professional Responsibility Module is responsible for receiving, documenting, referring, investigating, and reporting allegations of misconduct and/or harassment involving DHS personnel. Office of Professional Responsibility's mission is to promote the integrity of the DHS workforce by ensuring expeditious, fair, objective, and accountable review of allegations of misconduct and/or harassment.
- **Center for International Safety and Security (CISS) Module** – The Center for International Safety and Security Module is responsible for Foreign Access Management, Technical Surveillance Countermeasures, and Operations Security for the Department. It processes Foreign Activity Inquiries, Requests for Information, and Requests for Support.
- **Personal Security Division Special Actions Branch (PSD SAB) Module** – The Personal Security Division Special Actions Branch Module coordinates and tracks notifications submitted from other OCSO lines of business regarding employment suitability and security eligibility for DHS employees and contractors.
- **Insider Threat Operation Center (ITOC) Module** – The Insider Threat Operations Center Module serves as a repository for tracking and managing the workflows associated with the Insider Threat Operation Center's insider threat analysis, inquiry, and mitigation activities.

J-TIMS is a case management system initially used only by DHS OCSO, but now has expanded to other DHS Components such as the Federal Emergency Management Agency (FEMA), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Customs and Border Protection (CBP), Federal Law Enforcement Training Centers (FLETC), U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services (USCIS), and U.S. Secret Service (USSS). J-TIMS is an enterprise-ready system that logically partitions Component data from one another and allows other DHS Components to leverage the existing J-TIMS Modules.

J-TIMS is accessible only on the DHS network and uses Windows-integrated authentication. Modules are accessible using role-based access. Each module has tailored security groups and permissions, such as an admin and user groups. The records created within each module (i.e., cases, inquiries, investigations) are, by default, only accessible by those with login access to the appropriate owning module. These records can be explicitly shared across modules to appropriate system users/groups with access to J-TIMS based on their respective module's internal Standard Operating Procedure (SOP).

Reason for the PIA Update

In accordance with the DHS Directive System MD Number 0810.1, *The Office of the Inspector General*,[1] DHS Organizational Elements[2] (OE) are required to promptly advise the OIG of allegations of specific types of misconduct,[3] and when they become aware of any audit, inspection, or investigative work being performed or contemplated within their offices by or on behalf of an OIG from outside of DHS, the General Accountability Office (GAO), or any other law enforcement authority, unless restricted by law.

The OIG, while organizationally a Component of DHS, operates independent of the Department and all offices within it. OIG is authorized, among other things, to initiate, conduct, supervise, and coordinate audits, investigations, inspections, and other reviews relating to the programs and operations of DHS; and 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, rules, or regulations, a cause for suspension or debarment, mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety.

OIG reports directly to the Secretary of Homeland Security and has the authority to initiate,

[1] *See* 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.
[2] Organizational Elements are offices within DHS responsible for Investigations and Operations, Threat Management Operations, Enterprise Security Operations and Support, Headquarters Support, and Professional Responsibility or Internal Affairs.
[3] Identified in Appendix A of DHS MD 0810.1.

conduct, supervise, and coordinate audits, investigations, inspections, and other reviews related to programs and operations within DHS, including criminal and misconduct allegations reported by employees, contractors, and other individuals. This authority gives OIG the first right of refusal to investigate any reported allegations. The OIG reviews initial allegations to determine whether to exercise its right to conduct an investigation.

Such referrals are transmitted by the Organizational Element offices immediately upon receipt of the allegation, and the Organizational Element offices conduct no investigations before referral unless failure to do so would pose an imminent threat to human life, health, or safety, or result in the irretrievable loss or destruction of critical evidence or witness testimony. In such extraordinary situations, the OIG will be contacted as soon as practical, and all information and evidence collected by the Organizational Element office shall then be provided to the OIG as part of the Organizational Element referral.

The Organizational Element offices will initiate the investigation upon receipt of the allegation shall notify the OIG's Office of Investigations within five business days of such allegations. The OIG shall notify the Organizational Element offices if the OIG intends to assume control over or become involved in such an investigation, but absent such notification, the Organizational Element office shall maintain total responsibility for these investigations.

Any allegations received by the OIG that do not come within the categories specified in the Management Directive System, MD Number 0810.1, or that the OIG determines not to investigate will be referred within five business days of receipt of the allegation by the OIG to the appropriate Organizational Element office along with any confidentiality protections deemed necessary by the OIG.

In compliance with the Management Directive System, MD Number 0810.1, each reported event is triaged, and if it meets the OIG referral threshold, then it is manually reported to OIG through the public-facing DHS OIG Hotline website.[4] There are also circumstances where additional allegations are discovered during or at the end of an Investigation Operations Division investigation, Office of Professional Responsibility case, or Insider Threat Operations Center case that will require reporting to OIG. The OIG referral is then managed within emails and manually tracked in J-TIMS. OIG provides a confirmation email acknowledging the referral submission, including a case number for each referral. Once OIG has reviewed the referral, they will inform the Organizational Element office via email or through the OIG Liaison if OIG accepts or declines.

- If accepted, the initiating Organizational Element office will notate OIG's acceptance of the referral and halt any investigation activities, and provide them over to OIG.

[4] *See* https://www.oig.dhs.gov/hotline.

- If declined, the initiating Organizational Element office will refer the Reported Event to the appropriate J-TIMS module for investigation.

To streamline this process, J-TIMS will integrate with OIG's LEDX to automate the allegation referral process. Through J-TIMS, authorized users will submit allegations referrals to OIG through LEDX directly from the following Modules: Case Support Team, Investigations and Operations Division, Insider Threat Operation Center, and Office of Professional Responsibility. Once the referral is reviewed and processed, an Accepted or Declined response will be automated back from OIG through LEDX to J-TIMS. This process will be used rather than communicating through the OIG Hotline and email.

If OIG determines that an allegation referral it receives outside the J-TIMS workflow falls within the responsibility of another DHS Organizational Element office, OIG will refer the allegation/complaint along with supporting documents to that appropriate DHS Organizational Element office. Currently, the referral is reviewed then entered in J-TIMS as a Reported Event to be further investigated by the appropriate J-ITMS Module. This process will now be automated with LEDX, where complaint referrals will be received directly in J-TIMS, eliminating the email process.

Privacy Impact Analysis

Authorities and Other Requirements

The same legal authorities from the original J-TIMS Privacy Impact Assessment continue to provide coverage for these security-related activities. In addition, below are OIG-specific authorities:

- Inspector General Act of 1978; and
- Department of Homeland Security Management Directive System MD Number 0810.1 (6/10/2004), The Office of Inspector General.

In addition to the System of Records Notices (SORN) listed in the previous J-TIMS Privacy Impact Assessments, the following System of Records Notice applies to OIG activities:

- DHS/OIG-002 Investigative Records System,[5] which covers OIG's collection and maintenance of records related to alleged violations of criminal, civil, and administrative laws and regulations pertaining to DHS programs, operations, employees, contractors, and other individuals and entities associated with DHS.

The OIG information within the Case Support Team, Insider Threat Operation Center,

[5] *See* DHS/OIG-002 Investigative Records System, 86 Fed. Reg. 58292 (October 21, 2021), *available at* http://www.dhs.gov/system-records-notices-sorns.

Investigations and Operations Division and Office of Professional Responsibility modules is covered by the following retention schedules:

- Information in the Case Support Team and Insider Threat Operation Center module is maintained in accordance with General Records Schedule (GRS) 5.6, Security Records, for 25 years from the date of first reporting. If DHS deems a person "not of concern," the information will be destroyed three years after notification of death or five years after (1) the individual no longer has an active security clearance held by DHS, (2) separation or transfer of employment, or (3) the individual's contract relationship with DHS expires; whichever is applicable.
- Information in the Investigations and Operations Division and Office of Professional Responsibility Modules are maintained in accordance with General Records Schedule 5.6, Item 181 - Records filed with the record-keeping copy of the erroneously released records: Follow the disposition instructions approved for the released record copy or destroy six years after the erroneous release, whichever is later.
- Records filed separately from the record-keeping copy of the erroneously released records: TEMPORARY. Destroy six years after the erroneous release, but longer retention is authorized; General Records Schedule 5.6, Item 200 - TEMPORARY. Destroy three years after final investigation or reporting action or when three years old, whichever is later, but longer retention is authorized for business use; N1-563-08-4 - TEMPORARY. Cut-off at the end of the fiscal year when the case is closed. Destroy 20 years after the cut-off.

Characterization of the Information

J-TIMS will provide OIG with the full allegation details for the right of first refusal to investigate the allegation. J-TIMS will submit the following information to OIG when submitting allegation referrals for review:

- OIG Submission
    - IG Reference Number
    - Origin (Event Number, Investigation Operations Division Case Number or Office of Professional Responsibility Case Number)
    - IG Status
    - Date Submitted
- Reported Event
    - Event Number
    - Date Occurred

  - Description
- Investigations Operations Division Investigation
  - Case Number
  - Case Summary
  - Incident Location
- Office of Professional Responsibility Case
  - Case Number
  - Case Summary
  - Incident Location
- Insider Threat Operations Center Case
  - Case Number
  - Report of Findings
- DHS Persona[6] (Source, Subject, Witness, Co-Subject, Point of Contact)
  - Name
  - Business Address (past/present)
  - Email Address
  - Business Phone
  - Component
  - Position/Title
- Non-DHS Persona (Source, Subject, Witness, Co-Subject, Point of Contact)
  - Name
  - Business Phone
  - Email Address

The below data fields are provided back to J-TIMS through LEDX based on the OIG response:

[6] For more information on the Persona process, please see the original J-TIMS Privacy Impact Assessment, U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE JOINT-THREAT INFORMATION MANAGEMENT SYSTEM, DHS/ALL/PIA-084 (2020), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs (pp. 4-6).

- IG Case Number
- IG Action – Accept/Decline
- IG Response Required – Y/N
- IG Response Details
- Date Responded

When OIG deems an allegation to fall under one of the J-TIMS Modules for investigation, J-TIMS will receive the following OIG Complaint Referral Information for review and investigation:

- Case Details
    - Case Number
    - Received Date
    - Incident Date
    - Incident City
    - Incident State
    - Incident Zip
    - Affected Agency
    - Related Cases
    - Narrative
- Entity Details
    - Entity Type (Individual or Institution)
    - Entity Role (Subject, Victim, Witness or Complainant)
    - First Name
    - Last Name
    - Middle Initial
    - Institution Name
    - Address
    - City
    - State
    - Zip

- Email
- Phone
- DHS Employee (Y/N)
- Alias
- Agency

Information submitted to OIG is collected from individuals reporting potential allegations (criminal or administrative violations) captured within the Reported Event. Additional data collected by the Office of Professional Responsibility, Insider Threat Operations Center, or Investigations Operations Division analysts, investigators, contractors, and fact finders investigating the allegation can also be collected and submitted to OIG.

Since J-TIMS users leverage external databases such as LexisNexis and Clear and social media (when deemed appropriate), commercial data is sometimes collected as background information to verify addresses, identities, and contact information, identify illegal activities, identify possible witnesses, and for other investigative purposes that will generate a new referral to OIG.

Uses of the Information

OIG and OCSO will utilize the OIG LEDX to share allegation information rather than rely on the existing OIG Hotline or previous sharing processes. Allegation referrals will be shared by J-TIMS to OIG to determine if an OIG investigation is warranted, in accordance with Management Directive System, MD Number 0810.1. If the OIG accepts the allegations, then the Office of Professional Responsibility, Insider Threat Operations Center, or Investigations Operations Division will halt any investigation activities and hand off to OIG for the investigation. If the OIG declines the allegation, the allegation will be triaged to determine which module will conduct the appropriate investigation. The information received from OIG will be used to record, investigate, and resolve reports of misconduct, from the initial receipt of the allegation through the investigation process to its final disposition/adjudication.

Privacy Risk: There is a privacy risk that authorized J-TIMS users will access or use this information received from OIG for unauthorized purposes.

Mitigation: This risk is mitigated. Prior to gaining access to J-TIMS, all users receive training regarding the sensitivity of the investigative records and information, as well as restrictions on disclosure through the Privacy Act. Data entered into J-TIMS requires peer and supervisor review in accordance with the specific module owner's Standard Operating Procedures. Access to and actions taken by J-TIMS users are automatically recorded in the system's audit log and auditable in accordance with the specific module owner's Standard Operating Procedure.

Notice

This Privacy Impact Assessment and the applicable System of Records Notice outlined above provide public notice of this information's general collection, use, and maintenance. However, because J-TIMS is an investigatory case management system that collects and maintains sensitive information related to insider threat, security, misconduct, or criminal investigations, it is not always feasible or advisable to provide notice to specific individuals when their information is input into J-TIMS.

Notice of collection by the other federal agency systems and offices, including DHS, performing the original collection may be described in the individual Privacy Impact Assessments and System of Records Notices for those entities. Commercial databases and publicly available websites may provide their own notice as part of their own requirements.

Data Retention by the Project

The current version of J-TIMS does not include automation or rules related to information retention. In a future development phase, rules will be retroactively implemented based on retention policies for each module.

The retention period for the information collected and maintained in J-TIMS varies depending on the module. DHS-owned data is retained in accordance with the System of Records Notice for the underlying system from which the data is obtained.

The OIG information within the Case Support Team, Insider Threat Operation Center, Office of Professional Responsibility and Investigations and Operations Division modules is covered by the following:

- Information in the Case Support Team and Insider Threat Operation Center modules is maintained in accordance with General Records Schedule (GRS) 5.6, Security Records, for 25 years from the date of first reporting. If DHS deems a person "not of concern," the information will be destroyed three years after notification of death or five years after (1) the individual no longer has an active security clearance held by DHS, (2) separation or transfer of employment, or (3) the individual's contract relationship with DHS expires; whichever is applicable.
- Information in the Office of Professional Responsibility and Investigations and Operations Division modules is maintained in accordance with General Records Schedule 5.6, Item 181 - Records filed with the record-keeping copy of the erroneously released records: Follow the disposition instructions approved for the released record copy or destroy six years after the erroneous release, whichever is later. Records filed separately from the record-keeping copy of the erroneously released records: TEMPORARY. Destroy six years after the erroneous release, but longer retention is authorized; General Records

Schedule 5.6 Item 200 - TEMPORARY. Destroy three years after final investigation or reporting action or when three years old, whichever is later, but longer retention is authorized for business use; N1-563-08-4 - TEMPORARY. Cut-off at the end of the fiscal year when the case is closed. Destroy 20 years after the cut-off.

Privacy Risk: There is a risk that information may be retained longer than necessary.

Mitigation: This risk is partially mitigated. Currently, records must be removed manually. In accordance with the General Records Schedule described above and internal J-TIMS policies and procedures, annual reviews will be conducted to ensure records are appropriately removed. In the next J-TIMS phase of development, the system will allow for tagging any existing and new records within each module and automatically remove records based on the applicable retention rules associated with those tags.

Information Sharing

Only the required information outlined in Directive System MD Number 0810.1 will be shared between OIG and J-TIMS. However, no information is shared directly out of J-TIMS. Any investigation findings will be provided to OIG on formal letterhead memoranda.

Information is not generally shared outside of DHS as part of normal agency operations. However, information may be shared on a case-by-case basis. This is typically done through email, orally during briefings, interviews, official requests, and by telephone with other government entities, including law enforcement agencies and third parties with a need-to-know. The information shared depends on the nature, subject, status, and other factors unique to each investigation or information request; no general rule that applies to the data within J-TIMS. The sharing restrictions and responsibilities apply to the DHS Components and Divisions that own the information.

Privacy Risk: There is a risk that OIG information could be shared inappropriately.

Mitigation: This risk is mitigated. OIG information will be shared with other modules when sharing is aligned with the purpose for which the data was collected. All J-TIMS modules have Privacy Impact Assessment Updates that conform to the parent System of Record Notice, which address their potential sharing with external recipients. Sharing with external partners is manually reviewed and evaluated on a case-by-case basis.

Redress

Because J-TIMS may contain sensitive information, DHS has exempted certain records maintained within the system from access. However, individuals may seek access to their records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or the Judicial

Redress Act still may seek access to records consistent with the Freedom of Information Act unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. An individual may file a Privacy Act or Freedom of Information Act request via mail to the below address or file the request electronically at https://www.dhs.gov/foia:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Requests must be in writing and include the requestor's full name, current address, date and place of birth, country of citizenship or residency, and as much information as possible about the subject matter to facilitate the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "Submit a FOIA Request." 6 CFR part 5, Subpart B, provides the rules for requesting access to Privacy Act records maintained by DHS.

Auditing and Accountability

Access to J-TIMS is controlled via user roles and auditing. An OIG Admin user role was developed for each module to designate which user(s) can submit and manage OIG allegation referrals directly in J-TIMS. Module Supervisor and above roles will be able to view in a read-only capacity all OIG submissions for their respective component. Module Non-Supervisor roles (such as Investigator, Case Officer, Analyst, or Inquiry Official) will only be able to see the OIG submissions within their respective module.

Contact Official

Steven C. Dodd
Program Management Analyst
Office of the Chief Security Officer U.S. Department of Homeland Security
202-282-8433

Responsible Official

Sean Thrash
Director, Insider Threat Program
Office of the Chief Security Officer
U.S. Department of Homeland Security

Approval Signature

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

_____

Deborah Fleischaker
Chief Privacy Officer (A)
U.S. Department of Homeland Security
privacy@hq.dhs.gov