Privacy Impact Assessment Update

for the

Joint-Threat Information Management System (J-TIMS)

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

May 8, 2024

Homeland Security

Abstract

The Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO) is responsible for protecting DHS people, information, and resources against constantly evolving security threats. OCSO maintains the Joint-Threat Information Management System (J-TIMS) to meet this responsibility and manage information from across its Directorates (Threat Management Operations (TMO), Enterprise Security Operations and Support (ESOS), and Headquarters Support). DHS is conducting this Privacy Impact Assessment (PIA) Update to add a new module to J-TIMS for the Personnel Security Division (PSD) Special Actions Branch (SAB), which is situated within the Headquarters Support Directorate.

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 listed J-TIMS modules which 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.

J-TIMS supports OCSO activities from security intake and case initiation to closure, providing greater collaboration on investigative matters between Directorates. Currently, J-TIMS supports six modules:[1]

- **CST (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 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.
- **SIR (Security Incident Reporting) 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 (SSO) to conduct

[1] *See* 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.

inquiries and to arrive at the final determination on the security incident.

- **INV (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 on DHS personnel, information, and property. These investigations are predicated off allegations or information 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 (ROI) is completed, providing a means to manage workflows, serve as a central repository of corrective actions, and aid in the formation and generation of both management and analytical reports.
- **CFL (Cyber Forensic Laboratory) Module** – The Cyber Forensic Laboratory serves as a support function to the Investigations and Operations Division and other law enforcement and administrative investigative groups within DHS. The Cyber Forensic Laboratory conducts impartial cyber forensic examinations by employing industry standard best practices. This module is used as a solution to manage Cyber Forensic Laboratory cyber service requests, cases, and case evidence.
- **OPR (Office of Professional Responsibility) Module –** The Office of Professional Responsibility is responsible for receiving, documenting, referring, investigating, and reporting allegations of misconduct and/or harassment involving DHS personnel. The 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.
- **CISS (Center for International Safety and Security) Module –** The Center for International Safety and Security Module is responsible for Foreign Access Management, Technical Surveillance Countermeasures, and Operations Security for the Department. The Center of International Safety and Security Module will join J-TIMS to process Foreign Activity Inquiries, Requests for Information, and Requests for Support.

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 group and a user group. 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

DHS is updating this Privacy Impact Assessment to account for the Personnel Security Division's (PSD) Special Actions Branch (SAB) Module being added to J-TIMS. The PSD SAB sits within the Headquarters Support Directorate of OCSO, and per *DHS Instruction 121-01-001 (Organization of the Office of the Chief Security Officer)* is responsible for the implementation of enterprise policy and procedures and manages the administration of all aspects of the Personnel Security Program at DHS Headquarters to include security clearances, employment suitability determinations, and continuous evaluation of employees to ensure eligibility for employment.[2] PSD acts in accordance with Chapter 5 of *DHS Instruction 121-01-007-01, Suspension, Denial and Revocation of Access/Eligibility for Classified Information*.[3]

In accordance with Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive (SEAD) 3,[4] any information related to the adjudication of a security clearance is required to be reported to PSD SAB by individuals and other OCSO lines of business regarding employment suitability and security eligibility for DHS employees and contractors. The PSD SAB Module within J-TIMS will help streamline how PSD SAB receives this information from the following J-TIMS Modules: Investigation and Operations Division (INV), Security Incident Reporting (SIR), Insider Threat Operation Center (ITOC), and Office of Professional Responsibility (OPR). At the conclusion of an investigation, incident, or case, if the subject(s) meets the threshold and is found to have information that impacts their employment suitability and security eligibility, then the designated module users will create and submit a notification to PSD SAB from their respective module within J-TIMS. Designated module users are as follows:

- Security Incident Reporting Module: SIR Admins; Signature Authorities
- Investigations and Operations Module: ISD Admins, Supervisors, Case Agents
- Insider Threat Operations Center Module: ITOC Program Managers, Operations Branch Chiefs, Analyst Team Leads, Case Support Team Leads
- Office of Professional Responsibility: OPR Case Managers, Supervisors, Executive

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, INSTRUCTION, ORGANIZATION OF THE OFFICE OF THE CHIEF SECURITY OFFICER (September 3, 2008), *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt_instr_121_01_001_instruction_for_the_office_of_the_chief_security_officer.9.3.08.pdf.

[3] *See* DHS Instruction 121-01-007-01, Revision 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program, Chapter 5, Suspension, Denial and Revocation of Access/Eligibility to Classified Information, *available at* https://www.dhs.gov/sites/default/files/publications/InstructionHandbook121-01-007PersonnelSuitabilityandSecurityProgram.pdf.

[4] See OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SECURITY EXECUTIVE AGENT, *available at* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy.

Supervisors

The designated module users will decide how to share any applicable supporting documents with PSD SAB to support the results of their respective investigation, incident, or case, consistent with law and policy:

- **Security Incident Reporting Module:** The Security Incident Reporting Module will provide PSD SAB with the final signed Letter of Infraction, Letter of Violation, or Memorandum of Record.
- **Investigations and Operations Module:** The Investigations and Operations Module is within the Threat Management Operations Directorate. The Investigations and Operations Division (INV) will provide PSD SAB with a formal Notification Memo and any relevant approved Reports of Investigations (ROI) and/or Exhibits. Any sensitive investigation information will be redacted by the designated module user prior to submitting any information to PSD SAB.
- **Insider Threat Operational Center Module:** The Insider Threat Operational Center Module will provide PSD SAB with an approved Report of Findings.
- **Office of Professional Responsibility Module:** The Office of Professional Responsibility Module will provide PSD SAB a formal Memo of Findings or Disposition Notification Letter .

The information is provided within J-TIMS by the respective Investigations and Operations Division, Security Incident Reporting, and Insider Threat Operation Center Modules. PSD SAB will update their file accordingly or conduct the appropriate administrative investigation in the Integrated Security Management System (ISMS).[5] Once the file update and/or administrative investigation is completed within the Integrated Security Management System, PSD SAB will provide the final adjudication back to the requester within J-TIMS. The PSD SAB will not use J-TIMS as a case management system for their file updates and/or administrative investigations; this process will remain in the Integrated Security Management System. Therefore, only the final adjudication details will be provided back to the requester within J-TIMS.

The Adjudication information includes the following:

- Adjudication Decision – After the PSD SAB reviews the Notification, PSD SAB will complete an initial review to determine if any next steps are required.
- Adjudication Explanation – Provide any supplemental information regarding the

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED SECURITY MANAGEMENT SYSTEM (ISMS), DHS/ALL/PIA-038 (2011 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

Adjudication decision.

- Action Taken and Date of Action – This includes any action PSD SAB completed after their administrative investigation such as File Update, Continuous Evaluation, Warning/Advisement, Suspension, or Revocation; and the date when that action took place.

In addition, PSD SAB may receive referrals through Reported Events that require clearance action. The PSD SAB Module Owner will review a referral to determine if it falls within their scope and take the appropriate actions. An example of this appropriate action would be to determine if a file update in the employee's Integrated Security Management System profile requires an additional review to determine if PSD SAB should conduct an administrative investigation. Any file updates and/or administrative casework will still be performed within the Integrated Security Management System. Only the final adjudication details will be provided within J-TIMS to close out the Referral.

Privacy Impact Analysis

Authorities and Other Requirements

The same legal authorities discussed in the original J-TIMS Privacy Impact Assessment provide coverage for the security-related activities discussed above. In addition, below are PSD SAB specific authorities.

- Executive Order 12968, as amended, "Access to Classified Information," August 2, 1995;
- Title 5, United States Code (U.S.C.), Section 552(a), "Records maintained on individuals" [The Privacy Act of 1974, as amended];
- DHS Instruction 121-01-007-01 Chapter 8, ISMS – Safeguarding Personnel Security Records; and
- General Records Schedule 5.6: Security Management Records.

The System of Records Notice (SORN) that applies to PSD SAB activities is:

- DHS/ALL-023 Personnel Security Management System of Records,[6] which covers records obtained by OCSO for personnel security responsibilities.

[6] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 Fed. Reg. 8088 (February 23, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.

Characterization of the Information

Since PSD SAB will continue their casework in the Integrated Security Management System, the PSD SAB Module will only provide the high-level adjudication details back to the requester from their respective module in J-TIMS.

Entities specific to the PSD SAB Module include the following:

- PSD Notification:
  - Notification Number
  - Notification Status
    - Submitted
    - In Process
    - Completed
    - Pending Update
  - Reported Event
  - Subject of Investigation
  - Adjudication Decision
    - Undetermined
    - Non Actionable
    - Actionable Clearance Holder
    - Actionable Non-Clearance Holder
  - Adjudication Explanation
  - Action Taken
    - Reviewed and File Updated
    - Continuous Evaluation
    - Warning / Advisement
    - Suspension
    - Revocation
    - On Appeal
  - Date of Action

- Submitted Date
- In Process Date
- Completed Date
- Submitted By
- In Process By
- Completed By
- Update Reason

PSD SAB will review the information and/or results provided by the other J-TIMS modules and conduct an administrative investigation in the Integrated Security Management System.

Uses of the Information

The information received in the PSD SAB Module is used to record, refer, adjudicate, and resolve special and adverse actions that affect or have the potential to affect an individual's employment or clearance eligibility with DHS. This PSD SAB Module is used to streamline the process for providing adjudication information directly to the Investigation and Operations, Security Incident Reporting, and Insider Threat Operation Center Modules. PSD SAB will also use J-TIMS to receive and respond to Referrals from other J-TIMS Modules.

The PSD SAB Module will provide adjudication responses directly within the initial notification sent from the Investigation and Operations, Security Incident Reporting, Insider Threat Operation Center, and the Office of Professional Responsibility with the final disposition and disciplinary action, as applicable, of the DHS personnel. This system will provide the adjudication data used for aggregate reporting to management. Data includes total Adjudications and Actions taken (e.g., suspensions, revocations, reinstatements), associated timelines for that workflow, and referrals to and from other modules.

These reports are generated for statistical and performance-based purposes for managing special actions, adverse actions, and inquiries. Security specialists and investigators gather additional background information regarding individuals associated with a case. As part of the adjudicative process, information from subjects, complainants, witnesses, and third parties may be used for general contact purposes, as search terms in searchable public and non-public databases for information relating to the case, and for other investigative purposes.

The PSD SAB Module contains information only pertaining to the DHS HQ organizations. PSD SAB adjudicates clearances of all HQ employees, affiliated contracts, and some state and local individuals. Other OCSO sections include the following: Investigations Operations Division conducts DHS criminal investigations; Insider Threat assesses potential dangers to DHS from internal parties; Security Incident Reporting monitors security violations. These sections may

provide valuable information for clearance adjudication. Only PSD SAB personnel have roles and responsibilities in the PSD SAB Module.

Privacy Risk: There is a risk that authorized users will access or use information in the PSD SAB Module for unauthorized purposes.

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

Privacy Risk: There is a risk that information maintained in the PSD SAB Module may be accessed by another user that does not have a need-to-know.

Mitigation: This risk is mitigated. J-TIMS is a role-based system, limiting access to information based on the set permissions to the specific user role. Only the designated PSD SAB user groups (Security Specialist and Administrators) can access the PSD SAB Module. In addition, only designated users from Investigation and Operations, Security Incident Reporting, Insider Threat Operation Center, and Office of Professional Responsibility Modules can submit notifications to PSD SAB. Also, the PSD SAB Module has a designated module owner who submits user account requests to J-TIMS system administrators for account provisioning. J-TIMS users do not have access to a module or information within a module unless approved by the module owner and provisioned by an administrator.

Notice

This Privacy Impact Assessment update and the applicable System of Records Notice provide public notice of the general collection, use, and maintenance of information. Because J-TIMS is an investigatory case management system that collects and maintains sensitive information related to security or criminal matters or investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is input into the system. When PSD SAB security specialists interact with individuals in connection with an administrative investigation, those individuals are generally aware that their information will be recorded and stored by DHS. When individuals apply for a covered position, they complete and execute the Standard Form 86,[7] Questionnaire For National Security Positions General Release which states, "This authorization shall remain in effect so long as I occupy a national security sensitive position or require eligibility for access to classified information." Security specialists and investigators

[7] Standard Form (SF) 86, Questionnaire For National Security Positions, *available at* https://www.opm.gov/forms/pdf_fill/sf86.pdf.

also inform witnesses and subjects, when appropriate, that the information they provide will be recorded and stored. Additionally, Privacy Act rights are disclosed by the investigator at the beginning of any interview. Personnel Security Specialists and Investigators are DHS personnel authorized to review background investigations or gather information associated with background investigations.

Notice of collection by other federal agency systems and offices, to include DHS, performing the original collection of information that may be relevant to an investigation may be described in the individual Privacy Impact Assessments and System of Records Notices for those entities.

Data Retention by the Project

PSD SAB safeguards records according to applicable rules and policies, including all applicable DHS systems' security and access policies. In accordance with General Records Schedule 5.6, Item 180 and 181, records relating to personnel security and access clearances are destroyed one year after consideration of the candidate ends. Personnel security clearance files for people issued clearances are destroyed five years after the employee or contractor relationship ends. Records relating to alleged security violations or regarding security clearance files may be authorized for longer retention periods if required for business use.

Since PSD SAB Notifications are supplementing Investigation and Operations, Security Incident Reporting, Insider Threat Operation Center, and Office of Professional Responsibility cases, the retention policies for those notifications fall under the respective case/investigation file's retention requirements.

Privacy Risk: There is a risk that the PSD SAB Module will retain information longer than necessary.

Mitigation: This risk is mitigated. Records in the PSD SAB Module are removed manually following Standard Operating Procedures. In the next J-TIMS phase of development, the system will allow for the tagging of any existing and new records on an annual basis within each module and automatically remove records based on the applicable retention rules associated with those tags.

Information Sharing

Information in the PSD SAB Module is not shared outside of DHS as part of normal agency operations. However, such information may be shared on a case-by-case, need-to-know basis, through official U.S. government email, which is password protected, 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, in existing processes outside of J-TIMS. Further, as noted above, personally identifiable information is redacted if the individual

with whom the document is shared does not have a need-to-know the specific personally identifiable information. The actual information shared depends on the nature, subject, status, and other factors unique to each investigation or information request. Any disclosures are annotated in the J-TIMS record.

Privacy Risk: There is a risk that information in the PSD SAB Module could be shared inappropriately.

Mitigation: This risk is mitigated. Information maintained in the PSD SAB Module will be shared with peer modules when sharing is aligned with the purpose for which the information was originally 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. Information maintained in the PSD Module will not be exposed to external recipients unless through referral to other modules consistent with users' access roles and need-to-know. 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, an individual 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 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, and country of citizenship or residency, and as much information as possible about the subject matter of the request to facilitate the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under "Contact Information." 6 CFR part 5, Subpart B, provides the rules for requesting access to Privacy Act records maintained by DHS.

Auditing and Accountability

PSD SAB Module users have an official duty that requires knowledge of information regarding security clearances, employment suitability, determinations, continuous evaluation, and eligibility for employment for DHS employees and contractors. PSD SAB Module users will follow the PSD Standard Operating Procedures, and complete the required training (including annual privacy training). Additionally, users have received a copy of the J-TIMS Privacy Impact Assessment and corresponding updates.

Two types of user roles were assigned in J-TIMS for the PSD SAB Module: PSD SAB Supervisor and PSD SAB Security Specialist. The PSD SAB Supervisor role is for J-TIMS Administrators with complete access and oversight for the PSD SAB Module. The PSD SAB Security Specialist role will be assigned to individuals responsible for processing the PSD Notifications submitted from Investigation and Operations, Security Incident Reporting, Insider Threat Operation Center, and Office of Professional Responsibility.

Contact Official

Danielle Blue
Branch Chief, Special Actions Branch
Office of Chief Security Officer
U.S. Department of Homeland Security
danielle.blue1@hq.dhs.gov
(202) 281-5995

Responsible Official

Eric Bauer
Deputy Director, Personnel Security Division
Office of Chief Security Officer
U.S. Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

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