Privacy Impact Assessment

for the

Joint-Threat Information Management System (J-TIMS)

DHS Reference No. DHS/ALL/PIA-083(b)

February 10, 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 manage information from across its Directorates (Threat Management Operations (TMO), Enterprise Security Operations and Support (ESOS), and Headquarters Support) to support its mission. DHS OCSO is conducting this Privacy Impact Assessment (PIA) Update to add a new module to J-TIMS for the Insider Threat Operations Center (ITOC), which is situated within the Threat Management Operations 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 fulfil that mission. Each module in J-TIMS is part of a joint effort by the Threat Management Operations, Enterprise Security Operations and Support, and Headquarters Support Directorates to enable information sharing, referrals, and sending and receiving leads to initiate and support cases. The 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 prioritization when required.

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

- **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.
- **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 to conduct inquiries and make the final determination on the security incident.

[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.

- **IOD (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 the formation and generation of 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 employing 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 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 administrative group and a user group. The records created within each module (i.e., cases, inquiries, investigations, forensic examinations) are by default only accessible by the appropriate owning module and individuals with approved access to the respective module. These records can be explicitly shared across modules to appropriate system users/groups with access to J-TIMS, based on a "need to know" and the respective module's internal Standard Operating Procedure.

Reason for the PIA Update

This Privacy Impact Assessment is being updated to provide notice of the development of an Insider Threat Operations Center (ITOC) Module in J-TIMS. The ITOC sits within the Threat Management Operations Directorate of OCSO. Pursuant to Executive Order 13587, "*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*," the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and DHS Instruction 262-05-002, "*Insider Threat Program*," the DHS Insider Threat Program was established to prevent, detect, and mitigate the threat that an insider may use their authorized access, wittingly or unwittingly, to cause harm to the Department's mission, personnel, facilities, information, networks, and systems. These threats are manifested in espionage, domestic and international terrorism, unauthorized

disclosure, workplace violence, sabotage, and corruption in the form of support to transnational criminal and drug trafficking organizations. Within the DHS Insider Threat Program, the ITOC serves as the enterprise coordination and de-confliction hub for all insider threat matters across DHS and maintains a centralized insider threat analytic and response capability to electronically gather, integrate, review, assess, and respond to information with insider threat value concerning DHS personnel.

The J-TIMS ITOC Module will serve as a repository for tracking and managing the workflows associated with the ITOC's insider threat analysis, inquiry, and mitigation activities. Specifically, the J-TIMS ITOC Module will be used to enhance documentation and tracking of the following: initial intake and assessment of tips and referrals made to the ITOC; conduct of all inquiry activities in response to potential insider threat indicators; development of insider threat referrals to the appropriate DHS, Component, or other U.S. Government Department or Agency stakeholder office(s); analytic activities in support of stakeholder requests to leverage the capabilities of the ITOC; and de-confliction and tracking of all insider threat matters across DHS and its Components.

For more information about the DHS Insider Threat Program, please see DHS/ALL/PIA-052 Insider Threat Program (2015 and subsequent updates), available at https://www.dhs.gov/publication/dhs-all-pia-052-dhs-insider-threat-program.

Privacy Impact Analysis

Authorities and Other Requirements[2]

The same legal authorities from the original J-TIMS Privacy Impact Assessment provide coverage for the security-related activities discussed above. In addition, the following are ITOC-specific authorities:

- Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information;[3]
- Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs;[4]
- DHS Delegation of Authority 08503 (Aug. 10, 2012);

[2] Any authorities listed without citations are internal DHS policies and documents.
[3] Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 FR 63811 (October 7, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.
[4] Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012), *available at* https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.

- DHS Directive 262-05, Information Sharing and Safeguarding (Sept. 4, 2014);[5]
- DHS Instruction 262-05-002, "Insider Threat Program," (Oct. 1, 2019);
- DHS Instruction 262-05-002-01, "Insider Threat Information Sharing Guide," (Oct. 11, 2019);
- DHS Office of the Chief Security Officer, Insider Threat Program, SOP-002: ITOC Analytic Activities (Oct. 1, 2021);
- Office of the Director of National Intelligence, Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position;[6]
- DHS Directive 121-14, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (Sept. 17, 2018);[7]
- Intelligence Community Standard 500-27, Collection and Sharing of Audit Data;[8]
- Intelligence Community Standard 700-2, Use of Audit Data for Insider Threat Detection; and
- Intelligence Community Standard 703-02, Reporting Requirements for Individuals with Access to Sensitive Compartmented Information.

In addition to the System of Records Notices (SORN) listed in the original J-TIMS Privacy Impact Assessment, the DHS/ALL-038 Insider Threat Program System of Records Notice[9] specifically applies to ITOC activities.

ITOC safeguards records according to applicable rules and policies, including all applicable DHS databases' security and access policies. In accordance with General Records Schedule 5.6: Security Records (July 2017), Insider Threat (a) records pertaining to an "insider threat inquiry" are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat information" are destroyed when 25 years old; (c) insider threat user activity monitoring

[5] DHS Directive 262-05, Information Sharing and Safeguarding, *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_262-05-information-sharing-and-safeguarding.pdf.
[6] Office of the Director of National Intelligence, Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, *available at* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf.
[7] DHS Directive 121-14, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (Sept. 17, 2018), *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/security/mgmt-dir_121-14-report-requirements-personnel-access-classified-info_rev00.pdf.
[8] Intelligence Community Standard 500-27, Collection and Sharing of Audit Data, *available at* https://dni.gov/files/documents/FOIA/DF-2016-00213.pdf.
[9] DHS/ALL-038 Insider Threat Program System of Records, 85 FR 13914 (March 10, 2020).

data is destroyed no sooner than five (5) years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records are destroyed after seven (7) years, but longer retention is authorized if required for business use.

Characterization of the Information

The below data fields are included in the ITOC Module:

- ITOC Cases
  - Case Number
  - Case Type
  - Case Status
  - Work Status
  - Link to Reported Event
  - Subject (Link to Persona (i.e., person record) in J-TIMS)[10]
  - Case Predicate Narrative
  - OIG Complaint Number (if applicable)
  - Case Disposition
  - Primary & Alternate Assigned Analyst
  - Case Milestones (e.g., Dates of Initiation, Approval/Rejection, Closure)
- Insider Threat Risk Indicators
  - Risk Indicator Types
- Inquiry Related Records Checks
  - Record Checked
  - Date Checked
  - Subject (Link to J-TIMS Persona)
  - Findings Narrative

[10] 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).

- Requests for Information (RFI)
    - Request Number
    - Office
    - RFI Status
    - Point of Contact
    - Date Initiated
    - Response Narrative
- Referrals
    - Summary of Findings Narrative
    - Referral Number
    - Referral Office
    - Referral Date
    - Date Completed
    - Case Disposition
    - Personnel Security Division (PSD) Notifications (Linked through J-TIMS)
        - Notification Number
        - Notification Status
        - Subject (Linked to J-TIMS Persona)
        - Link to Reported Event
        - Submitted Date
        - Adjudicative Decision
        - Personnel Security Division Action Taken
        - Date of Action
- Support Requests
    - Request Number
    - Request Status
    - Link to Reported Event
    - Subject (Linked to J-TIMS Persona)

- Requester Information
  - Requester Name
  - Requester Title
  - Email
  - Phone
  - Agency
- Request Details
  - Request Date
  - Case Type
  - Special Handling Caveats Pertaining to the Case Details, such as For Official Use Only, or Law Enforcement Sensitive
  - Case Number Reference
  - Requested Assistance Narrative
  - Subject's Network Accesses
  - Search Channels
  - Request Description Narrative
- Office of the General Counsel (OGC) Details
  - OGC Reviewed
  - Attorney Advisor Name
  - Attorney Advisor Phone
- Support Request Milestones
  - Approved By
  - Approved Date
  - Rejected By
  - Rejected Date

In addition, the below data may be included in supporting documentation maintained as part of the ITOC's inquiry activities (e.g., background investigations forms such as Standard Forms 86, Reports of Investigation, Adjudications Worksheets, credit bureau reporting, results of criminal history and other indices checks) if needed in furtherance of the inquiry. Only data relevant to or

that supports specific allegations or insider threat indicators is queried and maintained as part of the ITOC's inquiry records.

- Individual's name and alias(es);
- Date and place of birth;
- Address;
- Open source information, including publicly available social media information related to the specific insider threat indicators justifying the inquiry activity;[11]
- Personal and official email addresses;
- Citizenship;
- Personal and official phone numbers;
- Driver's license number(s);
- Vehicle Identification Number(s);
- License plate number(s);
- Ethnicity and race;
- Current Employment and Performance Information;
- Work history;
- Education history;
- Contract information;
- Information on family members, dependents, relatives, and other personal contacts disclosed during a background or security clearance investigation;
- Passport number(s);
- DHS-held Travel records;
- Gender;
- Hair and eye color;
- Fingerprint information used for the purposes of identity verification and criminal history

[11] The ITOC limits its social media activity to efforts that are reasonably likely to identify publicly available information related to the specific insider threat indicators justifying the inquiry activity. This may include reviewing the publicly available posts, images, biographic information, and geolocation data associated with the subject's social media presence.

queries during a background or security clearance investigation

- Other physical or distinguishing attributes of an individual, such as height, weight, and scar or tattoo characteristics, that may be included in criminal history records;
- Medical information;
- Access control pass, credential number, or other identifying number(s);
- Media obtained through authorized procedures, such as CCTV footage; and
- Any other information provided to obtain access to DHS facilities or information systems.
- Records relating to the management and operation of the DHS physical, personnel, and communications security programs, including:
  - Completed standard form questionnaires issued by the Office of Personnel Management;
  - Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
  - Current and former clearance status(s);
  - Other information related to an individual's eligibility for access to classified information;
- Criminal history records;
- Polygraph examination results;
- Logs of computer activities on all DHS IT systems or any IT systems accessed by DHS personnel;
- Nondisclosure agreements;
- Document control registries;
- Courier authorization requests;
- Derivative classification unique identifiers;
- Requests for access to sensitive compartmented information;
- Records reflecting personal and official foreign travel;
- Facility access records;
- Records of contacts with foreign persons; and
- Briefing/debriefing statements for special programs, sensitive positions, and other related

information and documents required in connection with personnel security clearance determinations.

- Reports of investigations or inquiries regarding security violations or misconduct, including:
  - Individuals' statements or affidavits and correspondence;
  - Incident reports;
  - Drug test results;
  - Investigative records of a criminal, civil, or administrative nature;
  - Letters, emails, memoranda, and reports;
  - Exhibits, evidence, statements, and affidavits;
  - Inquiries relating to suspected security violations;
  - Recommended remedial actions for possible security violations;
  - Personnel files containing information about misconduct and adverse actions; and
- Any information related to the management and operation of the DHS Insider Threat Program, including:
  - Documentation pertaining to factfinding or analytical efforts by Insider Threat Program personnel to identify insider threats to DHS resources, personnel, property, facilities, or information;
  - Records of information technology events and other information that could reveal potential insider threat activities;
  - Intelligence reports and database query results relating to any person who has or who had authorized access to any DHS facility, information, equipment, network, or system;
  - Information obtained from the Intelligence Community, law enforcement partners, and from other agencies or organizations about individuals and/or organizations conducting official business with DHS, or with a nexus to DHS personnel, that are known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat;
  - Information provided by subjects and individual members of the public; and
  - Information provided by individuals who report known or suspected insider threats.

The ITOC collects information obtained from the following sources: (1) software that monitors DHS users' activity on U.S. Government computer networks; (2) information supplied by

individuals to the Department or by the individual's employer; (3) information provided to the Department to gain access to DHS facilities, information, equipment, networks, or systems; (4) publicly available information obtained from open source platforms, including publicly available social media information related to the specific insider threat indicators justifying the inquiry activity; (5) any departmental records for which the Insider Threat Program has been given authorized access; and (6) any federal, state, tribal, local government, or private sector records for which the Insider Threat Program has been given authorized, lawful access. The ITOC also receives tips and leads by other means, such as email or telephone. The ITOC may receive a tip or lead from any party, including members of the public.

Privacy Risk: There is a risk that information manually entered into the ITOC Module may be inaccurate.

Mitigation: This risk is mitigated. In addition to the original mitigations for data entry, the ITOC Module also employs an internal review process, which includes a weekly review of all open inquiry activities led by the Operations Branch Chief and Analyst Team Leads, to ensure analytic sufficiency, compliance with policies and standard operating procedures, and data integrity and accuracy of the information analysts enter into the ITOC Module. In addition, data visualization and metrics capabilities of J-TIMS further assist the Operations Branch Chief and Analyst Team Leads with identifying and rectifying any discrepancies or inaccuracies with the information in the ITOC Module.

Privacy Risk: There is a risk that more information is maintained in the ITOC Module than necessary.

Mitigation: This risk is partially mitigated. ITOC personnel use remote structured behavioral threat assessment and psychological risk evaluation tools that guide the collection and analysis of records that are relevant in determining whether insider threat indicators or behaviors are apparent. ITOC personnel receive continuous training on the application of these tools from a contracted clinical psychologist and subject matter expert in detecting and mitigating insider risks, which further supports limiting only that information which is deemed necessary as part of an inquiry to be included in the ITOC Module.

Uses of the Information

The information collected in the ITOC Module is used to record, assess, track, and resolve potential insider threat concerns reported to, or developed by, the ITOC. The information within the ITOC Module will also facilitate a formal, holistic assessment of insider threat indicators or behaviors from the initial lead, through the entire inquiry and referral process, and to the final disposition or mitigating action(s) taken by a stakeholder office (i.e., law enforcement, counterintelligence, security, human resources, information assurance, or an individual's assigned duty office/location). The data within the ITOC Module also provides analysts, Team Leads,

supervisors, program leadership, and the Insider Threat Oversight Group (ITOG - consisting of Office of the General Counsel, Privacy Office, and Office for Civil Rights and Civil Liberties representatives) with an aggregate view of data and trends associated with insider threat reporting and indicators through unique querying and visualization capabilities. These reports (or dashboards) are generated primarily for performance-based indicators of effectiveness and timeliness, and overall efficacy of the ITOC mission. The information collected and maintained within the ITOC Module may also be used by analysts as search terms for additional information relevant to the subject of an inquiry activity.

Privacy Risk: There is a risk that authorized personnel will use information in the ITOC Module for unauthorized purposes.

Mitigation: This risk is mitigated. Prior to gaining access to J-TIMS and the ITOC Module, all users receive training regarding the sensitivity of the investigative records and information, as well as restrictions on disclosure stipulated by the Privacy Act, the applicable System of Records Notice, and DHS policy. Access to and actions taken by ITOC Module users are automatically recorded in the system's audit log and are auditable by team leads and supervisors.

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

Mitigation: This risk is mitigated. DHS mitigates this risk by using user roles and role-based account access. The ITOC Module is a role-based system, limiting access to information based on the set permissions to the specific user role. Each module has a designated module owner. These module owners submit user account requests for their respective modules 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 and the System of Records Notice outlined above provide public notice of the general collection, use, and maintenance of this type of information. Annual training and periodic messaging by the Department also inform personnel of the Insider Threat Program.

However, because J-TIMS and the ITOC Module are investigatory case management systems that collect and maintain sensitive information related to insider threat, security, or criminal investigations, it is not always feasible or advisable to provide notice to specific individuals at the time their information is input into J-TIMS.

Notice of collection by the other federal agency systems and offices, to include 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.

Privacy Risk: There is a risk that individuals may not know their ITOC-related information is maintained in J-TIMS.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment, in conjunction with the applicable System of Records Notices, provides notice about the information maintained within and used by the ITOC Module. However, because of the investigative nature of the system, and specifically the Insider Threat Program, it may not be appropriate to provide notice to individuals who are the subject of an insider threat activity or investigation that their information is in J-TIMS.

Data Retention by the Project

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

The retention period for the information collected and maintained in the ITOC Module varies depending on the type of data. DHS-owned data is retained in accordance with the System of Records Notice for the underlying system from which the data is obtained. The ITOC safeguards records according to applicable rules and policies, including all applicable DHS databases' security and access policies. In accordance with General Records Schedule 5.6: Security Records (July 2017), Insider Threat (a) records pertaining to an "insider threat inquiry" are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat information" are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data is destroyed no sooner than five (5) years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records are destroyed after seven (7) years, but longer retention is authorized if required for business use.

Privacy Risk: There is a risk that the information in the ITOC Module will be retained longer than approved retention periods.

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

Information Sharing

The ITOC shares information with appropriate stakeholder offices internal and external to DHS when analytic activity reasonably indicates that a DHS employee, contractor, or detailee may be an insider threat, or when analytic activity indicates that a subject DHS employee, contractor, or detailee may have committed acts that violated federal statutes or DHS rules, regulations, policies, or procedures. However, no information is shared directly out of J-TIMS. The ITOC documents its findings on formal letterhead memoranda and may refer matters for appropriate action to the following offices (depending on the nature of the concern or violation): OCSO, DHS Office of Inspector General, Component Internal Affairs or Security Offices, Component Insider Threat Programs, appropriate DHS management officials, other Federal departments or agencies, or state and local law enforcement authorities with appropriate jurisdiction.

Any information shared with other federal departments or agencies, or state and local law enforcement authorities is shared in a manner consistent with the relevant routine use identified in the Insider Threat Program System of Records Notice. This dissemination is approved by a team lead and supervisor and is reviewed by the Office of the General Counsel before any external sharing may occur. If approved, a record of the disclosure will be formally documented in J-TIMS and include, at a minimum: the requesting agency, authorized purpose for sharing, the DHS approving authority, the data to be disseminated, and any dissemination or re-dissemination conditions.

Privacy Risk: There is a risk that information in the ITOC Module may be inappropriately shared with external recipients.

Mitigation: This risk is mitigated. No information is shared directly from J-TIMS. The ITOC documents its findings on formal letterhead memoranda and shares information through existing processes outside of J-TIMS. ITOC information may be shared with recipients outside DHS when sharing is aligned with the purpose for which the information was originally collected. More specifically, external sharing is governed by the DHS/ALL-038 Insider Threat Program System of Records and the other applicable System of Records Notices listed in Section 1.2 of the original J-TIMS Privacy Impact Assessment, which define the purpose for which the information was collected, and with whom and under what circumstances the information can be shared. ITOC analysts receive annual training addressing the privacy and the safeguarding of information through IT security and integrity awareness. The branch chief of each module approves all sharing prior to any external dissemination and retains an accounting of all external sharing for auditing purposes.

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 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 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 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.

Given the sensitive nature of the ITOC, a robust redress process to permit access, review, and correction of information and referrals cannot be provided. This lack of direct access and a formal redress mechanism poses a risk to individual privacy. However, given the heightened sensitivity of and potential harm to national security and law enforcement activities supported by the ITOC, such access is infeasible. Although individuals do not have a formal mechanism for access or redress, DHS has internal mechanisms to correct inaccuracies and protect against abuse through the information system security protections and controls described above. Additionally, DHS reviews all such requests for information on a case-by-case basis

Auditing and Accountability

ITOC personnel have extensive experience in security, counterintelligence, and law enforcement and are required to sign DHS Insider Threat Program-specific non-disclosure agreements acknowledging the sensitivities of the information and records, including information maintained within the J-TIMS ITOC Module, to which they have access, and the implications of unauthorized disclosure or mishandling of this information. As part of their onboarding, and routinely thereafter, all ITOC personnel are advised of, and trained on, the ITOC's analytic standard operating procedures, including those governing J-TIMS and all inquiry and case management-related activities. Furthermore, all ITOC personnel complete assigned mandatory annual privacy training and are provided a copy of this Privacy Impact Assessment for reference.

The following user roles were developed within the J-TIMS ITOC Module with permissions commensurate with their job functions: Analyst, Analyst Team Lead, Case Support Team Lead, Operations Branch Chief, and Program Manager. The Analyst and Case Support Team Leads and Operations Branch Chief roles maintain permissions to ensure oversight and quality control of all inquiry records that are initiated, elevated, referred, or closed, as well as the specific activities conducted by the Analyst roles. The Program Manager role maintains broad read-only permissions to all ITOC inquiry records to ensure full oversight and transparency. Analysts maintain permissions to document all inquiry activities to which they have been assigned as the Lead or Alternate Analyst; however, they maintain limited read-only access to all other records within the ITOC Module.

Responsible Official

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer
Department of Homeland Security

Sean Thrash
Director, Insider Threat Division
Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

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

_____

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