Privacy Impact Assessment
for the

Joint-Threat Information Management System (J-TIMS)

DHS/ALL/PIA-084

April 24, 2020

Contact Point
Sean Thrash
Director, Insider Threat Program
Office of the Chief Security Officer
(202) 447-5316

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Office of the Chief Security Officer (OCSO) is delivering an enterprise-wide security solution to protect DHS people, information, and resources against constantly evolving security threats. OCSO accomplishes this goal with various divisions specializing in different lines of business. Under OCSO, the divisions consist of the following: Internal Security Division (ISD), Security Incident Reporting (SIR), Personnel Security Division (PSD), and Cyber Forensic Laboratory (CFL). To efficiently manage security case-related information across these divisions, OCSO has developed the Joint-Threat Information Management System (J-TIMS).

Overview

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 and deployment of multiple case management systems that caused disjointed records management and difficulty in sharing case-related information within OCSO. Over time, it has become apparent that without a centralized solution for managing the intake and tracking the lifecycle of security-related events, OCSO's lines of business could potentially be missing important connections between security events. Lacking such a system, OCSO requires a solution to help expose, mitigate, and quickly resolve security threats in a timely manner.

Therefore, OCSO has developed the Joint-Threat Information Management System (J-TIMS) in collaboration with the Office of the Chief Information Officer (OCIO) Solutions Development Directorate (SDD) Business Systems Branch (BSB). J-TIMS uses an agile methodology for the development and implementation of the application.[1] In order to support OCSO activities across the enterprise, J-TIMS is a configured line of business application with minimal customization built on a Microsoft Dynamics 365-based solution deployed in the DHS HQ Government Community Cloud (GCC). The first phase of J-TIMS's agile development will generally involve only Headquarters (HQ) activities.[2]

[1] J-TIMS is an enterprise system that will allow DHS Components to use the system. The system will logically partition Component data from each other. Each Component will only have access to its respective data. All role-based access controls and sharing policies would align with what is outlined in this PIA. An Appendix will be added to this PIA and updated as additional Components are added. The Appendix will identify any further differences or privacy risks not already described in the PIA.

[2] Depending on the nature of OCSO reporting requirements and policies, the J-TIMS HQ partition may maintain information on activities handled by DHS Component Security Offices or that involve personnel from multiple Components. This may include significant security incidents or those in which an HQ employee is a party to an investigation of a Component employee, for example.

J-TIMS will support OCSO activities from security intake and case initiation to closure, providing greater collaboration on investigative matters between divisions. The initial implementation of J-TIMS will occur on the DHS Unclassified Network (A-LAN) and will include four modules: [3]

- **CST (Case Support Team) Module** – The CST is primarily responsible for the intake of all reported security events in accordance with approved guidelines. The CST triages reported events to determine the responsible office within which the event falls. In coordination with various analyst teams, the CST identifies and creates referrals that are then sent to the appropriate DHS Component or OCSO Division. The CST coordinates the handover of reported events and any other related information to the appropriate office to potentially be worked further as a case. The CST resides within the DHS Insider Threat Program (ITP) as it serves as the central hub for all security reporting for DHS HQ. As such, the DHS ITP relies on the CST to successfully coordinate with the various investigative offices within DHS HQ to enhance the overall visibility of various security efforts across OCSO and the Department.[4]
- **SIR (Security Incident Reporting) Module** – The SIR is responsible for safeguarding and protecting Classified National Security Information. The SIR was created to outline security standards and best practices for handling classified information to all employees within the Department. The SIR aims to provide guidance to the DHS enterprise in formulating and ultimately implementing an operational and effective security incident program. Consistent with Executive Order 13526,[5] this program is responsible for promptly actioning and producing comprehensive reports regarding reported security incidents involving the mishandling, possible compromise, or compromise of classified information. The SIR Module assists in this mission by providing a centralized tool for managing all security incidents. In addition, it streamlines the process of assigning Special

[3] These modules are specific to the HQ partition of J-TIMS. Components will generally have the same modules; however, depending on the significance of any differences in Component partitions, this PIA will either be updated or the differences will be described in the Component's Appendix entry.
[4] As part of the intake process, CST may determine that a security-related event should be referred to ITP. Insider Threat case or investigation information will not be maintained in J-TIMS. All Insider Threat information is maintained separately by the DHS Insider Threat Operations Center (ITOC). However, if a reported event becomes an Insider Threat case/investigation, that intake information will still be maintained by J-TIMS. For more information about the ITP, *see* DHS/ALL/PIA-052 DHS Insider Threat Program, *available at* https://www.dhs.gov/privacy.
[5] Executive Order 13526, *Classified National Security Information* (December 29, 2009), available at https://www.archives.gov/isoo/policy-documents/cnsi-eo.html.

Security Officers (SSO) to conduct inquiries and the final determination of the security incident.

- **ISD (Internal Security Division) Module** – The ISD conducts impartial, independent, and thorough criminal and administrative investigations on DHS personnel, information, and property. These investigations are predicated off allegations or information of employees or contractors engaged in criminal or administrative misconduct. The ISD 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. Furthermore, the ISD Module provides the ability to update records once the matter has been fully adjudicated.

  Many criminal and administrative investigations involve interviewing individuals to ascertain information that may assist in the investigation. Interviews are a planned conversation, the purpose of which is to obtain, confirm, explain, or supplement information pertinent to the investigation. Policies and procedures are in place to address the individual's rights and obligations that vary depending on the type of investigation, and on whether the interviewee is a federal employee, as well as other circumstances (e.g., bargaining unit employee). To safeguard the rights of interviewees, ISD is responsible not only for determining the facts associated with allegations of misconduct, but equally responsible for the preservation and protection of the civil and administrative rights afforded to all subjects and witnesses encountered during the investigation, irrespective of their status as DHS employees, other public service workers, or members of the public. All participants in investigative interviews conducted by ISD are afforded specific notifications informing them of their rights and obligations. The requirements differ depending on the nature of the criminal or administrative investigation.

  The ISD Module collects, compiles, and delivers accurate and real-time information on case status, investigative activities, ROIs, ROI Exhibits (Memorandum of Activity (MOA) and sworn statements), and legal or administrative disposition actions. The module provides ISD with 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 CFL serves as a support function to ISD and other law enforcement and administrative investigative groups within DHS. The CFL conducts impartial cyber forensic examinations by employing industry standard best practices. This module is used as a solution to manage CFL cyber service requests, cases, and case evidence.

The CFL receives Cyber Service Requests internally within OCSO, specifically ISD, other DHS offices (e.g., DHS Office of Inspector General), Components, and occasionally from agencies outside of DHS. The requests are reviewed and approved by the branch chief or designee, which then initiates a CFL case. The CFL takes appropriate action in either processing provided evidence or obtaining evidence from the DHS network.

CFL maintains a case with all associated evidence records within the CFL Module. A CFL examiner is assigned to the case and begins the examination process based on the type of evidence. Evidence intake includes the creation or transfer of the chain of custody and this information is maintained throughout the case. The forensic examination process is completed on a CFL-dedicated network that is outside of J-TIMS. Updates to the status of the case and the final report will be notated and uploaded in the CFL Module. Upon completion of a case, the CFL will mark the case as "closed" in the module. A completed physical case file is also stored in the CFL secure evidence room. At time of completion, the most up to date chain of custody information will be uploaded to the CFL Module.

J-TIMS is accessible only on the DHS network and uses Windows integrated authentication. Modules are accessible using role-based access to the following DHS Component-based user groups:

- Case Support Team (CST Admins)
- Security Incident Reporting (SIR Admins, Signature Authorities [ISD Director], Inquiry Officials [Special Security Officers], Branch Chiefs)
- Internal Security Investigations (ISD Admins, Supervisors (Special Agent in Charge), Case Agents)
- Cyber Forensics Lab (CFL Admins, Investigators)

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 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). The sharing of these records across J-TIMS modules is recorded in the internal audit log. Logically spanning all modules are Personas, Reported Events, Referrals, and Dashboards.

A **Persona** refers to a person of interest within the context of J-TIMS. This persona record can be tied to other module records in the system as needed. For example, a persona could be identified in the system as a witness or source of a reported event or the subject of an investigation.

Reported Events are objective accountings of security-related events observed and reported to DHS. CST enters the details of these events as a new reported event record, then triages the new reported event record and creates referrals to the appropriate module(s) within J-TIMS. This review process generally includes the input of additional information into the reported event record.

Referrals are notifications sent to module owners to inform them that there may be a response required by the recipient. There are two types of referrals:

1. Notification Referrals – Provide awareness to the recipient
2. Action Referrals – Expected engagement from the recipient

An example of the intake process would be a DHS employee reporting a potential security-related incident to the CST, which would then document the incident as a reported event in J-TIMS. After the CST conducts its initial analysis it sends the reported event, if appropriate, as a referral to the responsible module owners in J-TIMS. The module owners would review the referral to determine if it falls within their scope to be considered for action and, if necessary, conduct an investigation or inquiry.

Dashboards allow users to quickly access reported events, case information, and/or common tasks. System dashboards are specific to each module and corresponding user roles. Dashboards can consist of a collection of lists and charts; for example, a list of all open cases assigned to a J-TIMS user.

The J-TIMS team has partnered with the Trusted Identity Exchange (TIE)[6] team to integrate with the Integrated Security Management System (ISMS)[7] to populate DHS persona field data. Since ISMS is the authoritative source for DHS personnel security records, much of the personal information included in a persona record is queried from ISMS and displayed in a read-only format for J-TIMS users. The J-TIMS team uses TIE services to perform a lookup against ISMS persona data in order to add DHS personas into J-TIMS. Personas are only added when relevant to a Reported Event.

The J-TIMS team developed a custom user interface allowing J-TIMS users to perform a search against ISMS persona data. Through the user interface, users will be able to search, identify, and select the appropriate DHS persona to be imported into the system when needed and relevant to a Reported Event, Case, Investigation, or Inquiry. If an existing J-TIMS DHS persona is selected, then a check will be made through the TIE service to get the latest real-time data refresh

[6] *See* DHS/ALL/PIA-050 DHS Trusted Identity Exchange, *available at* https://www.dhs.gov/privacy.
[7] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

from ISMS. J-TIMS users are not able to edit any of the data imported from ISMS and any data updates come directly from ISMS.

After selecting a persona, the J-TIMS user is responsible for updating any remaining persona information required to properly conduct the inquiry or investigation by the appropriate OCSO Division. For example, an ISD investigator conducting an investigation regarding a particular subject enters information collected during the investigation about the subject into the subject's persona record in J-TIMS. Information specific to the ISD investigation itself remains in the subject's persona record, but access to that information is limited to only those J-TIMS users that can view ISD investigation information based on their security role.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

DHS is authorized to collect J-TIMS information pursuant to the following:

1. 6 U.S.C. § 341(a)(6), Under Secretary for Management;
2. 28 U.S.C. § 535, Investigation of Crimes Involving Government Officers and Employees; Limitations;
3. 40 U.S.C. § 1315, Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property;
4. By the regulations found at 5 CFR parts 731, 736, and 1400; and 32 CFR part 147;
5. Executive Order 12829 - National Industrial Security Program;[8]
6. Executive Order 12968 - Access to Classified Information (as amended);[9]
7. Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;[10]

[8] Executive Order 12829 - National Industrial Security Program, 58 FR 3479 (January 6, 1993), *available at* https://www.govinfo.gov/content/pkg/WCPD-1993-01-11/pdf/WCPD-1993-01-11-Pg17.pdf.
[9] Executive Order 12968 - Access to Classified Information, 60 FR 40245 (August 2, 1995), *available at* http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf.
[10] Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, 73 FR 38103 (June 30, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-07-02/pdf/08-1409.pdf.

8. Executive Order 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust;[11]
9. Executive Order 13526 - Classified National Security Information;[12]
10. Executive Order 13549 - Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities;[13]
11. Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information;[14]
12. Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs;[15]
13. DHS Delegation of Authority 08503, Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer;
14. DHS Delegation 12000, Chief Security Officer;
15. DHS Directive 121-01, Office of the Chief Security Officer;[16]
16. DHS Directive 262-05, Information Sharing and Safeguarding;[17]
17. DHS Directive 11052, Internal Security Program;[18] and

---

[11] Executive Order 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, 74 FR 4111 (January 16, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-01-22/pdf/E9-1574.pdf.
[12] Executive Order 13526 - Classified National Security Information, 75 FR 707 (December 29, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf.
[13] Executive Order 13549 - Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities, 75 FR 51609 (August 18, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-08-23/pdf/2010-21016.pdf.
[14] 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.
[15] 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.
[16] DHS Directive 121-01, Office of the Chief Security Officer, *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/security/mgmt-dir_121-01-chief-security-officer_revision-02.pdf.
[17] 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.
[18] DHS Directive 11052, Internal Security Program, *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/security/mgmt-dir_md-11052-internal-security-program.pdf.

18. DHS Instruction 262-05-01, Insider Threat Program.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/ALL-038 Insider Threat Program System of Records Notice (SORN)[19] covers all records and information used by DHS Insider Threat Program (ITP) related to the management and operation of DHS programs to safeguard DHS resources and information assets. This includes the intake information maintained in J-TIMS that may be referred to the ITP and potentially becomes part of an Insider Threat case or investigation.

The DHS/ALL-023 Personnel Security Management SORN[20] covers records obtained by OCSO for Personnel Security responsibilities. This covers the information associated with Personas and other security-related information collected during the course of investigations and inquiries by module owners.

The DHS/ALL-020 Internal Affairs SORN[21] covers all activities and information collected by Internal Security Investigations. This covers the information associated with criminal, civil, and administrative investigations.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. Microsoft Dynamics 365, the platform on which J-TIMS is hosted, has been granted an Authority to Operate (ATO). A system security plan (SSP) has been completed as a requirement for the ATO package.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Each J-TIMS module owner has different retention requirements according to its mission:

The CST Module retention schedule is:

- Until a CST referral is accepted, information in the CST 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

[19] DHS/ALL-038 Insider Threat Program System of Records, 85 FR 13914 (March 10, 2020).
[20] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[21] DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014).

or transfer of employment, or (3) the individual's contract relationship with DHS expires; whichever is applicable.[22]

- Once a CST referral is accepted by a J-TIMS module, that record falls under the accepting module's retention schedule (listed below).

The ISD and CFL retention schedules are:

Record	File Plan Number	Disposition Number	Instructions
Criminal Investigation Case Files. Includes Cyber and Evidence Case Files.	DAA-0563-2019-0009	N1-563-08-4 Item 2	TEMPORARY. Cut-off at the end of the fiscal year when the case is closed. Destroy 20 years after the cut off.
Information Release Violation Investigations. Includes Cyber and Evidence Case Files.	N1-305-109-18	GRS 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 6 years after the erroneous release, whichever is later. Records filed separately from the record-keeping copy of the erroneously released records: TEMPORARY. Destroy 6 years after the erroneous release, but longer retention is authorized if required by business use.
Investigative Files. Includes Cyber and Evidence Case Files.	N1-401-121-05	GRS 5.6, Item 200	TEMPORARY. Destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.
Non-Referral Files. Includes Cyber and Evidence Case Files.	N1-115-045-06	N1-563-08-4-3	TEMPORARY. Destroy when 5 years old.

The SIR retention schedule is:

[22] This aligns with the Insider Threat retention requirements as intake information maintained in J-TIMS may be referred to the ITP and potentially becomes part of an Insider Threat case or investigation. For more information about the ITP, *see* DHS/ALL/PIA-052 DHS Insider Threat Program, *available at* https://www.dhs.gov/privacy.

- Pursuant to GRS 5.6, Item 181 and Item 200, records relating to alleged security violations are destroyed five years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use. Personnel security clearance files for people issued clearances are destroyed five years after 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.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

J-TIMS does not collect standardized information directly from members of the public, and therefore, is not subject to the requirements of the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

J-TIMS requires information from various sources to perform its mission to safeguard DHS resources and information assets. J-TIMS collects the following types of information in different modules:

- Common entities shared across all modules:
    - **DHS Persona (Source, Subject, Witness, Co-Subject, Point of Contact)**
        - Name
        - Alias
        - Data of Birth
        - Foreign Born (Y/N)
        - Clearance Level
        - Employee Type
            - Federal Employee
            - Federal Detailee
            - Contractor
            - Other (Non-DHS Personas)

        - Position/Title
        - GS Level
        - Person Handle
        - Email Address
        - Business Phone
        - Business Address (past/present)
        - DHS Network and Access Privileges
        - Component
        - Sub Component
        - Office
        - Supervisor
    - **Non-DHS Persona (Source, Subject, Witness, Co-Subject, Point of Contact)**
        - Name
        - Employee Type
            - Other
        - Foreign Born (Y/N)
        - Business Phone
        - Email Address
    - **Reported Event**
        - Event Number
        - Description
        - Reported By (Persona in J-TIMS)
        - Reporting Method (e.g., phone, email)
        - Date Occurred
        - Date Reported
        - Person of Interest (Persona in J-TIMS)
        - Anomalous Behavior Details
        - Misconduct (Criminal/Non-Criminal) Details
        - Security Concern Details
- Information related to Internal Security Division's (ISD) criminal and administrative investigations:
    - **ISD Investigation**
        - Case Number
        - Case Title
        - Case Type

- Case Status
- Case Resolution
- Link to Reported Event
- Subject (Persona in J-TIMS)
- Subject Type (i.e., DHS Persona, Non-DHS Persona)
- Reported Date
- Case Summary
- Incident Location
- Allegation Synopsis

- **ISD Investigation Report of Investigation (ROI)**
  - Case Number
  - Report Number
  - ROI Status
  - ROI Update Reason
  - Report Type
  - Report Status
  - Topic
  - Narrative
  - Synopsis
- **ISD Investigation Exhibit**
  - Exhibit Type
  - Exhibit Detail
  - Exhibit Status
  - Activity Type
  - Activity Detail
  - Case Number
  - ROI
  - Narrative
  - Enclosure Details

- Information related to Security Incident Reporting (SIR) report of incidents, security violations, or misconduct
  - **SIR Incidents**
    - Case Number
    - Case Status
    - Component/Office

        - Discovered/Reported By (Persona in J-TIMS)
        - Self-Reported (Y/N)
        - Date of Occurrence
        - Date of Discovery
        - Subject (Persona in J-TIMS)
        - Incident Location
        - Incident Type Description
        - Incident Classification
        - Incident Validated
        - Non-Validation Explanation
        - Classified Information Secured (Y/N)
        - Unsecured Explanation
        - Narrative
        - Work Status
        - Additional Classification Markings
        - Root Cause
        - Findings
        - Recommendation
        - Compromise Determination
        - Incident Determination
        - Incident Closed On
- Information collected related Cyber Forensics Lab (CFL) service requests and associated cases:
    - **CFL Service Request**
        - Request Number
        - Request Status
        - Request Date
        - Case Type
        - Overall Classification
        - Case Reference Number
        - Requester
        - Title
        - Agency
        - Email Address
        - Address
        - Phone Number
        - Supervisor Name

- Supervisor Title
- Type of CFL Services Requested
  - Cell Phone / Device Forensics
  - Computer Forensics Examination
  - Data Recovery
  - Video Forensics / Image Clarification
- Media to be Examined
  - Cell Phone / Device
  - Forensic Image Files
  - Computer / Hard Disk Drive
  - Optical Media
  - Removable Storage Device
  - Other
- Incident Detail Search Criteria
- Search Authority
  - Administrative
  - Consent
  - Search Warrant
  - Other
- Critical Completion Date
- Critical Completion Justification
- Enclosures
  - Copy of Agency Evidence / Chain of Custody Form
  - Copy of Agency ROI or Incident Report
  - Copy of Written Consent
  - Copy of Search Warrant
  - Other

- **CFL Case**
  - Case Number
  - Case Type
  - Case Priority
  - Customer
  - Subject (Persona in J-TIMS)
  - External Case
  - Description
  - Date Received
  - Date Closed

- **CFL Case Evidence**
  - Case Number
  - Evidence Number
  - Evidence Type
  - Make
  - Model
  - Serial Number
  - Property Barcode
  - Document Number
  - Location
  - Archival Location
  - Date Archived
  - Description
  - Evidence Status
  - Date Received
  - Forensic Imaging
  - Processing
  - Examination
  - Reporting
  - Recent Inventory Date
  - Date Closed
  - Findings

Additionally, J-TIMS maintains information about DHS personnel who are assigned a case/investigation. This includes contact information about investigators, examiners, supervisors, etc. These roles and titles may be slightly different across the different modules.

2.2 What are the sources of the information and how is the information collected for the project?

J-TIMS will reference information from other DHS systems (e.g., ISMS and U.S. Custom and Border Protection's (CBP) Automated Targeting System (ATS)[23]), other federal agency systems (e.g., Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC)[24]), commercial and publicly available databases and websites (e.g., Lexis/Nexus), and individuals. This information may be ingested directly into J-TIMS (as is the case with data from ISMS) or manually entered by J-TIMS users during or after investigations, further research, other system or database checks, and interviews.

[23] *See* DHS/CBP/PIA-006 Automated Targeting System, *available at* https://www.dhs.gov/privacy.
[24] *See* https://www.fbi.gov/file-repository/pia-ncic.pdf/view.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. J-TIMS users will perform external checks during the course of their investigations using commercial sources and publicly available data sources, to include social media, when deemed appropriate. Commercial data is sometimes collected as background information to verify addresses, identities, and contact information; to identify illegal activities; to identify possible witnesses; and for other investigative purposes. This information is included in J-TIMS when relevant to an investigation. Commercial sources used by OCSO include subscriptions to law enforcement databases, such as LexisNexis and CLEAR.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of data is dependent on several factors depending on the source of the data. For example, J-TIMS is dependent on ISMS, the DHS authoritative source for DHS personnel security records, through the TIE, to accurately populate persona information. There are no other system-to-system connections with J-TIMS, so data from other federal agencies, checks of commercial or publicly available databases and websites, and information gathered during interviews or upon intake is manually entered into the system by J-TIMS users.

However, J-TIMS users are required by policy to alert data owners if records in an underlying system of record are identified as inaccurate. Additionally, as the source systems for other federal agency data or commercial data aggregators correct information, queries of those systems would reflect the corrected information once also corrected by the J-TIMS user.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information manually entered by J-TIMS users may be inaccurate.

Mitigation: This risk is mitigated. For persona creation, J-TIMS partnered with the TIE to receive authoritative personnel data from ISMS. These information fields are read-only in J-TIMS. This ensures the core biographic data is not manually entered and thus, accurate. For information that is manually entered into J-TIMS by users, the data is peer-reviewed by a team lead or supervisor before being finalized and included in any referral or formal reports. This ensures that information is not only accurate, but adheres to the mission and purpose of J-TIMS.

Privacy Risk: There is a risk that more information is maintained in J-TIMS than necessary.

Mitigation: This risk is mitigated. OCSO worked with the DHS Privacy Office to determine the minimal amount of information required to conduct case management through J-TIMS. This includes limiting the data imported from ISMS via the TIE. Additionally, OCSO personnel and investigators are trained on the sensitivity of the investigative techniques, information, and records.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The information collected in J-TIMS is used to record, investigate, and resolve suspected security events, from the receipt of an allegation, through the investigative process, and to the final disposition or discipline. The system also provides data used for aggregate reporting to management. J-TIMS provides enhanced querying and sorting capabilities, which enable routine and ad-hoc reports using primary data record types. These reports are generated for statistical and performance-based purposes for managing investigations and inquiries. Investigators gather additional background information regarding individuals associated with a case. As part of the investigative 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.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. Neither J-TIMS nor the end users will use the platform to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

During the first phase of J-TIMS development, users will be comprised of OCSO employees and counterintelligence employees on detail to the Insider Threat Operations Center (ITOC) from the Office of Intelligence and Analysis (I&A). Other DHS Components or federal agencies will not have access to J-TIMS. However, J-TIMS is being developed as an enterprise solution, so as new Components begin to use J-TIMS, the appropriate personnel will be given access. An Appendix will be added to this PIA and updated as additional Components are added to J-TIMS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that authorized users will use information in J-TIMS 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 SOPs. 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 SOP.

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

Mitigation: This risk is mitigated through the use of user roles and role-based account access. J-TIMS 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.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This PIA itself, as well as the SORNs outlined above, provide public notice of the collection, use, and maintenance of this type of information. Because J-TIMS is an investigatory case management system that collects and maintains sensitive information related to security or criminal investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is input into the system. When investigators interact with individuals in connection with an investigation, however, those individuals are generally aware that their information will be recorded and stored. Investigators also inform witnesses and subjects, when appropriate, that the information they provide will be recorded and stored.

Notice of collection by the other federal agency systems and offices, to include DHS, performing the original collection may be described in the individual PIAs and SORNs for those entities. Commercial databases and publicly available websites may provide their own notice as part

of their own requirements.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The other federal agency systems from which J-TIMS draws information through investigation include law enforcement, security, and intelligence systems that may collect information directly from individuals, providing notice at the time of collection. Those agencies may be required to provide notice by statutory mandate, or the information is collected under a law enforcement or intelligence authority. As such, individuals may not have an opportunity to decline to provide the required information, opt out, or consent to uses.

Depending on the nature of the investigation, interviewees and witnesses may be offered the opportunity to consent and request confidentiality. Confidentiality may be extended depending on the applicable laws and regulations.

4.3 Privacy Impact Analysis: Related to Notice

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

Mitigation: This risk is not fully mitigated. This PIA, in conjunction with the applicable SORNs, provides some notice about the information maintained and used within J-TIMS. However, because of the investigative nature of the system, it may not be appropriate to provide notice to individuals who are the subject of an investigation that their information is in J-TIMS.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The current version of J-TIMS does not include any automation or rules related to information retention. In the next phase of development, rules will be retroactively implemented based retention policies for each module, as defined below.

The CST Module retention schedule is:

- Until a CST referral is accepted, information in the CST module is maintained in accordance with 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.

- Once a CST referral is accepted by a J-TIMS module, that record falls under the accepting module's retention schedule (listed below).

The ISD and CFL retention schedules are:

Record	File Plan Number	Disposition Number	Instructions
Criminal Investigation Case Files. Includes Cyber and Evidence Case Files.	DAA-0563-2019-0009	N1-563-08-4 Item 2	TEMPORARY. Cut-off at the end of the fiscal year when the case is closed. Destroy 20 years after the cut off.
Information Release Violation Investigations. Includes Cyber and Evidence Case Files.	N1-305-109-18	GRS 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 6 years after the erroneous release, whichever is later. Records filed separately from the record-keeping copy of the erroneously released records: TEMPORARY. Destroy 6 years after the erroneous release, but longer retention is authorized if required by business use.
Investigative Files. Includes Cyber and Evidence Case Files.	N1-401-121-05	GRS 5.6, Item 200	TEMPORARY. Destroy 3 years after final investigation or reporting action or when 3 years old, whichever is later, but longer retention is authorized for business use.
Non-Referral Files. Includes Cyber and Evidence Case Files.	N1-115-045-06	N1-563-08-4-3	TEMPORARY. Destroy when 5 years old.

The SIR retention schedule is:

- Pursuant to GRS 5.6, Item 181 and Item 200, records relating to alleged security violations are destroyed five years after close of case or final action, whichever occurs sooner, but longer retention is authorized if required for business use. Personnel security clearance files for people issued clearances are destroyed five years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

5.2 Privacy Impact Analysis: Related to Retention

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

Mitigation: This risk is not mitigated. Currently, records must be removed manually. In the next J-TIMS phase of 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.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

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 actual information shared depends on the nature, subject, status, and other factors unique to each investigation or information request; there is not a general rule that applies to the data within J-TIMS. The sharing restrictions and responsibilities are applicable to the DHS Components and Divisions that own the information.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Any sharing of PII outside of the Department is compatible with the original collections and purposes listed in the SORNs of the source entity. Generally, however, information is not shared with outside agencies, with an exception being for law enforcement, intelligence, or national security purposes.

For example, during the course of an investigation or inquiry, investigators to share information with a federal, state, or local law enforcement agency. In this situation, the module owner would share the minimal amount of information necessary to the outside entity to further the inquiry or investigation. This information sharing is this example would be compatible with Routine Use G of the DHS/ALL-020 Internal Affairs.

6.3 Does the project place limitations on re-dissemination?

J-TIMS data shared with agencies external to DHS must first be approved for dissemination by that module owner's branch chief and reviewed by the Office of the General Counsel (OGC) before any external sharing may occur. If approved, the data is then formally entered into a Memo for the Record (MFR) format and recorded in J-TIMS. This MFR will 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. Once completed, the J-TIMS data may then be shared with a requesting agency if the data would serve a law enforcement, intelligence, or national security purpose.

6.4 Describe how the project maintains a record of any disclosures outside the department?

J-TIMS itself does not share information outside the Department directly. Any external sharing 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 branch chief of each module approves all sharing prior to any external dissemination and retains an accounting of all external sharing for auditing purposes, in accordance with current sharing practices.

6.5 Privacy Impact Analysis: Related to Information Sharing.

Privacy Risk: There is a risk that information in J-TIMS may be inappropriately shared with external recipients.

Mitigation: This risk is mitigated. J-TIMS information may be shared with recipients outside DHS when sharing is aligned with the purpose for which the information was collected. More specifically, external sharing is governed by the DHS/ALL-020 Internal Affairs SORN, as well as the other SORNs listed in Section 1.2, which define the purpose for which the information was collected, and with whom and under what circumstances the information can be shared.

System users receive annual training addressing the safeguarding of information through IT security and integrity awareness, as well as privacy 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.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

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 his or her 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 JRA still may seek access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her record, he or she may mail the request to the following address:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, SW
STOP-0655
Washington, D.C. 20528

These requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite 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.

Furthermore, DHS reviews all such requests for information on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, DHS will release information in accordance with the procedures and points of contact published in the applicable SORN.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The data accessed by J-TIMS users from other federal agency systems may be corrected by means of the processes described in the PIAs or SORNs applicable to those systems. DHS data

may be corrected as outlined in the SORNs in Section 1.2. Individuals may also submit Privacy Act requests as described in Section 7.1 above.

Because J-TIMS many times draws upon outside sources for its data, any changes to source system records (including the addition or deletion of source system records) are reflected during an inquiry or investigation. J-TIMS users are responsible for the integrity and confidentially of the data they input. Should erroneous information be entered, the user is required to correct his or her entry immediately upon determining it is incorrect.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures for correcting their information through the SORNs listed in Section 1.2, which cover the underlying systems from which J-TIMS accesses information.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to access, correct, and amend records about themselves given the law enforcement and investigatory nature of J-TIMS.

Mitigation: This risk cannot be fully mitigated. Given the nature of internal investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective investigation procedures, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

However, this risk is partially mitigated because by policy and pursuant to published SORNs, all requests for access, correction, and amendment of Privacy Act-covered records are evaluated by DHS on a case-by-case basis, regardless of exemption.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Microsoft Dynamics 365 provides an out of the box audit log feature that records every action performed by J-TIMS users. The audit logs are security trimmed based on J-TIMS user roles. Only authorized J-TIMS users can access the audit logs. On a retroactive basis, should an incident occur, logs are reviewed post-incident.

J-TIMS will be deployed in the DHS HQ Government Community Cloud (GCC), a Federal Risk and Authorization Management Program (FedRAMP)-compliant hosting location, in an environment that is exclusive to DHS use. J-TIMS will be further modified to comply with all existing DHS information assurance requirements. J-TIMS will be entirely isolated from any other Microsoft Dynamics 365 applications.

J-TIMS program/system managers oversee the implementation of sufficient security controls to mitigate the risk of compromise, unauthorized disclosure, and unauthorized acquisition of data containing PII. Any access to PII is restricted with an appropriate application of security controls. DHS Personnel who access, use, or disseminate PII without proper authorization may be subject to disciplinary action, including possible dismissal, as well as any penalties authorized by law. DHS personnel are obligated to report any suspected or confirmed breach immediately to a DHS supervisor, Component help desk, privacyhelp@dhs.gov, or the Component Privacy Officer/PPOC.[25]

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project?

All J-TIMS users are required to take annual DHS privacy training. Users who do not complete the required specialized annual training lose access to DHS Network. Additionally, other systems that OCSO personnel may also have access to may require additionally privacy and security training. Depending on the OCSO Division, personnel may also be required to complete training regarding the sensitivity of the investigative techniques, information, and records.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

J-TIMS 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.

However, information can also be shared across modules when appropriate, such as referral or CFL service request.

[25] All DHS employees may refer to the DHS Privacy Incident Handling Guidance online at https://www.dhs.gov/publication/privacy-incident-handling-guidance.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

The information shared will depend on the nature, subject, status, and other factors unique to each investigation or information request. Information sharing is done on a case-by-case basis as described in Section 6.0 of this PIA. Information sharing is not system-to-system, other than the TIE-ISMS relationship previously discussed, and will be shared through email, briefings, interviews, and telephone with other government entities, including law enforcement agencies and third parties with a need-to-know and as appropriate. Any new system-to-system connection, new uses of J-TIMS information, or new access by additional organizations will be reviewed in collaboration with the DHS Privacy Office and appropriate Component Privacy Office.

Responsible Officials

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

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

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

APPENDIX A: Federal Emergency Management Agency (FEMA)

((Updated June 23, 2023)

In October 2019, the Federal Emergency Management Agency (FEMA) Office of the Administrator established the Office of Professional Responsibility (OPR).[26] FEMA OPR is responsible for receiving, documenting, referring, investigating, and reporting allegations of misconduct and/or harassment involving FEMA personnel. FEMA OPR's mission is to promote the integrity of the FEMA workforce by ensuring expeditious, fair, objective, and accountable review of allegations of misconduct and/or harassment. In order to meet this mandate, FEMA OPR requires a technology solution. After looking at available systems in use throughout Department, as well as Commercial off the Shelf (COTS)/Government off the Shelf (GOTS) products, it was determined that the Joint-Threat Information Management System (J-TIMS) created for DHS Office of the Chief Security Officer (OCSO) closely met the needs of FEMA OPR.

FEMA OPR will work with the Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) Solutions Development Directorate (SDD) Business Systems Branch (BSB) to develop FEMA's own iteration of the ISD (Internal Security Division) Module within J-TIMS. FEMA will also use the J-TIMS Case Support Team (CST) Module, where FEMA's data will be logically partitioned from any other Component data or access.

FEMA's Module

FEMA OPR ensures expeditious, fair, and objective follow up and resolution of all allegations of employee misconduct and harassment and assists FEMA in building a culture that reflects the agency's core values of compassion, fairness, integrity, and respect. FEMA OPR conducts impartial, independent, and thorough administrative investigations on FEMA personnel. These investigations are predicated off allegations of personnel engaged in administrative misconduct.[27] The FEMA Module maintains the capability to track allegations of misconduct from receipt of the allegation through the adjudication process.

Many investigations involve interviewing individuals to ascertain information that may assist in the investigation. Policies and procedures are in place to address the individual's rights and obligations that vary depending on the type of investigation, and on whether the interviewee is a federal employee, as well as other circumstances (e.g., if the individual is a bargaining unit employee). To safeguard the rights of interviewees, FEMA OPR is responsible not only for determining the facts associated with allegations of misconduct, but equally responsible for the preservation and protection of the civil and administrative rights afforded to all subjects, witnesses,

[26] *See* FEMA Delegation FD-106-13, *Delegation of Authority to the Office of Professional* Responsibility, and FEMA Directive #112-13, *Office of Professional Responsibility*, on file with the FEMA Privacy Office.
[27] The J-TIMS ISD Module tracks both criminal and administrative misconduct. The FEMA Module will only track administrative misconduct handled by FEMA OPR.

and complainants encountered during the investigation, irrespective of their status as FEMA employees, other public service workers, or members of the public. All participants in investigative interviews conducted by FEMA OPR are afforded specific notifications informing them of their rights and obligations.

The FEMA Module collects, compiles, and delivers accurate and real-time information on case status, investigative activities, Report of Investigations (ROIs), ROI exhibits, and administrative disposition actions. The module provides FEMA OPR with 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.

Additionally, FEMA has a need to utilize the Security Incident Reporting (SIR) Module to help track security events and incidents. As part of the Enterprise SIR initiative, FEMA will be configured to leverage the SIR Module as-is, following the same processes and roles outlined by DHS HQ. FEMA's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined in at a later time.

Data Elements

In addition to the data elements outlined in Section 2.1 of this Privacy Impact Assessment (PIA), the FEMA Module will also collect the below information.[28]

- The following additions to the existing **DHS Persona**:[29]
  - Employee Type;[30]
    - Permanent Full-Time;
    - Cadre of On-Call Recovery Employees;
    - Reservist; and
    - Local Hire.
  - Name of Contracting Company (if a contractor); and
  - 2nd Level Organization Code.
- The following additions to the existing ISD-related case data elements:
  - Case Details
    - Investigative Lead Office
    - Region
    - Disaster Number

[28] SORN coverage for the information collected in the FEMA Module is covered by DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 Fed. Reg. 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[29] This DHS Persona data is fed from the DHS Trusted Identity Exchange (TIE) like the other DHS Persona data discussed in the PIA.
[30] These are additional employee types specific to FEMA given its unique emergency response function.

- Anti-Harassment Program (AHP) Determination Date
- AHP Designation
- DHS Office of Inspector General (OIG) Information
  - OIG Referred Status
  - Date Submission
  - OIG Case Status
  - Date of Response
- Disposition Date
- Close Date

- Offense
  - Offense(s)
  - Disposition(s)
- Referrals (to document referrals made outside J-TIMS)[31]
  - Referral Type
  - Date of Referral
  - Date of Notice
  - Office Referral Sent To
  - Offense(s)
  - Action(s)
  - Deciding Official

Uses of Information

Although FEMA is creating its own module within J-TIMS, the FEMA Module is very similar to the ISD Module explained earlier in the PIA. The biggest exception is that FEMA OPR only manages administrative, rather the criminal investigations as well.

Access controls will be implemented consistent with those outlined in the PIA above. The role-based access to the FEMA Module include the following roles: Case Manager, Supervisor, Executive Supervisor, Investigator, and Analyst.

Redress

The redress procedures listed in the PIA above are the same. However, because this is FEMA personnel and data, the contact point for such procedures is different. If an individual would like to file a Privacy Act or Freedom of Information Act (FOIA) request to view their record, they may mail the request to the following address:

Information Management Division/Disclosure Branch

[31] FEMA uses referrals to track the outcome of an investigation. In the event that the investigation was referred to another FEMA office, this section manages the conclusion of the actions/outcomes of the referral office so that it can be accurately tracked/closed in J-TIMS.

Federal Emergency Management Agency
500 C St. SW
Washington, D.C. 20472
Or by email to: fema-foia@fema.dhs.gov

Privacy Risks

Privacy Risk: There is a risk that more information will be collected in the FEMA Module as it differs slightly from the J-TIMS ISD Module and involves additional data elements.

Mitigation: This risk is mitigated. OCSO, as the system owner, worked with the DHS Privacy Office, FEMA Privacy Office, and FEMA OPR Team, as the business owner, to determine the minimal amount of information required to conduct OPR case management through J-TIMS. Prior to accessing J-TIMS, FEMA OPR employees must receive training on the appropriate use of the system. FEMA OPR Investigators also receive specific direction through FEMA directives and instructions that address the privacy interests in investigative materials. J-TIMS only allows FEMA OPR Investigators to provide information for the cases assigned to them. Data entered into J-TIMS is subject to managerial reviews, who have access and permissions to all FEMA case files, to ensure accuracy and adherence to applicable laws, regulations, and polices governing the rights and privacy of those involved in the investigation. FEMA OPR personnel and investigators are trained on the sensitivity of the investigative techniques, information, and records, DHS employees receive annual training addressing the safeguarding of information through IT security and integrity awareness, as well as privacy awareness.

Privacy Risk: There is a risk personnel without a need-to-know will be able to view FEMA data now that it is in the same system as OCSO data.

Mitigation: This risk is mitigated. OCSO has implemented the same role-based access controls for the FEMA Module that are in place for all other modules within the system. That means that access to information is limited based on the set permissions to the specific user role. Users will not have access to a module or information within a module unless approved by the module owner and provisioned by an administrator. Additionally, access to and actions taken by J-TIMS users are automatically recorded in the system's audit log, which is regularly reviewed to ensure the proper levels of control are in place.

APPENDIX B: Cybersecurity and Infrastructure Security Agency (CISA)

(Updated February 28, 2024)

The Cybersecurity and Infrastructure Security Agency (CISA) Office of the Chief Security Officer

(OCSO) has a need to have a centralized system to help track security events/incidents, misconduct allegations and potential insider threat matters. CISA will be configured to join J-TIMS application to support their security efforts. CISA will be leveraging four (4) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ and FEMA. CISA's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined in at a later time.

CISA will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a CISA Office or have been reported by CISA Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information
- Office of Professional Responsibility (OPR) Module – Investigations of allegations of misconduct and harassment by CISA Personnel
- Insider Threat Operations Center (ITOC) Module – Repository for tracking and managing the workflows associated with the ITOC's insider threat analysis, inquiry and mitigation activities

APPENDIX C: United States Secret Service (USSS)

(Updated June 23, 2023)

The United States Secret Service (USSS) has a need to have a centralized system to help track Security Incidents. As part of the Enterprise SIR initiative, USSS will be configured to leverage two (2) J-TIMS Modules as-is; following the same processes and roles outlined by DHS HQ. USSS' data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

USSS will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a USSS Office or have been reported by USSS Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information

APPENDIX D: U.S. Customs and Border Protection (CBP)

(Updated June 23, 2023)

The United States Customs and Border Protection (CBP) has a need to have a centralized system to help track Security Events and Incidents. As part of the Enterprise SIR initiative, CBP will be configured to leverage two (2) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ. CBP's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

CBP will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a CBP Office or have been reported by CBP Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information

APPENDIX E: Federal Law Enforcement Training Centers (FLETC)

(Updated June 23, 2023)

The Federal Law Enforcement Training Centers (FLETC) has a need to have a centralized system to help track Security Events and Incidents. As part of the Enterprise SIR initiative, FLETC will be configured to leverage two (2) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ. FLETC's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

FLETC will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a FLETC Office or have been reported by FLETC Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information

APPENDIX F: U.S. Immigration and Customs Enforcement (ICE)

(Updated June 23, 2023)

The United States Immigration and Customs Enforcement (ICE) has a need to have a centralized system to help track Security Events and Incidents. As part of the Enterprise SIR initiative, ICE will be configured to leverage two (2) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ. ICE's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

ICE will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a ICE Office or have been reported by ICE Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information

APPENDIX G: Transportation Security Administration (TSA)

(Updated June 23, 2023)

The Transportation Security Administration (TSA) has a need to have a centralized system to help track Security Events and Incidents. As part of the Enterprise SIR initiative, TSA will be configured to leverage two (2) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ. TSA's data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

TSA will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a TSA Office or have been reported by TSA Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information

APPENDIX H: U.S. Citizenship and Immigration Services (USCIS)

(Updated June 23, 2023)

The United States Citizenship and Immigration Services (USCIS) has a need to have a centralized system to help track Security Events and Incidents. As part of the Enterprise SIR initiative, USCIS will be configured to leverage two (2) J-TIMS Modules As-Is; following the same processes and roles outlined by DHS HQ. USCIS' data will be logically partitioned from any other Component data or access in J-TIMS. At this time, Components cannot share data with each other, any cross-component data sharing will be defined at a later time.

USCIS will be utilizing the following Modules:

- Case Support Team (CST) Module – Intake for all security-related events that occur at a USCIS Office or have been reported by USCIS Personnel
- Security Incident Reporting (SIR) Module – Incident inquiries involving the mishandling, possible compromise, or compromise of classified information