Privacy Impact Assessment

for the

Joint-Threat Information Management System (J-TIMS)

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

March 15, 2023

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. To achieve this, 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). DHS OCSO is conducting this Privacy Impact Assessment (PIA) Update to discuss adding information from the Center for International Safety and Security (CISS), within the Threat Management Operations Directorate, to the J-TIMS.

Overview

The primary mission of DHS is to prevent terrorism and enhance security, including the mitigation of risks and threats against the U.S. Government. Within DHS, OCSO's mission is to lead the collaborative security program to safeguard the Department's people, information, and property 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 of the modules in J-TIMS is part of a joint effort within the Threat Management Operations, Enterprise Security Operations and Support, and Headquarters Support Directorates to enable information sharing, referrals, and sending and receiving of leads to 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 security events in accordance with approved guidelines. The Case Support Team triages reported events to determine the responsible office within which the event falls. In coordination with various analyst teams, the Case Support Team identifies and creates referrals that are then sent 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

[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.

and make the final determination on the security incident.

- **Investigations and Operations Division (within the Threat Management Operations Directorate)) Module** – The Investigations and Operations Division conducts impartial, independent, and thorough criminal and administrative investigations related to security incidents involving DHS personnel, information, or property. These investigations are predicated on allegations against or information about employees or contractors engaged in criminal or administrative misconduct. The Investigations and Operations Division Module maintains the capability to track allegations of criminal or administrative misconduct from receipt of the allegation until the Report of Investigation 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 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 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 their respective module's internal Standard Operating Procedure.

Reason for the PIA Update

DHS is updating this Privacy Impact Assessment to account for the Center for International Safety and Security (CISS) Module being added to J-TIMS. The CISS Division sits within the Threat Management Operations Directorate of OCSO, and pursuant to DHS Instruction 121-01-001 *Organization of the Office of the Chief Security Officer*) is responsible for Foreign Access Management, Technical Surveillance Countermeasures, and Operations Security for the Department.[2]

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

As part of Phase 1 of CISS being integrated into J-TIMS, the CISS Division Operations Branch (OPs) will be joining J-TIMS to process Foreign Activity Inquiries, Requests for Information, and Requests for Support. CISS OPs identifies, analyzes, exploits, and mitigates foreign access and adversary security risks and threats to DHS and its components (personnel, critical information and infrastructure, funding programs and projects, information technology systems and networks, facilities, and operations) and other federal government agencies to support their law enforcement and national security functions, enhancing U.S. National Security. CISS OPs conducts internal and/or external investigations, inquiries, or audits related to foreign risks or threats where neglect, action, or inaction could cause inestimable damage to national security.

CISS OPs will use the J-TIMS CISS Module to intake, route, and track requests, including foreign activity inquiries, requests for information, and requests for support, which are initially received by email via DHS unclassified or classified networks. CISS OPs will review and triage all requests to ensure they: 1) clearly articulate the basis and purpose for the request; 2) fall within CISS' authority; 3) relate to an authorized mission; 4) comply with existing policies; 5) can be satisfied through CISS' existing accesses, resources, and processes; 6) identify a requestor with a valid "need to know" who is authorized to receive and collect the requested information; 7) provide the requestor's name, agency, and contact information; 8) provide the classification and priority level (routine, priority, or urgent); and 9) are furnished with as much detail, information, and/or identifiers with which to assist CISS in responding.[3]

Types of CISS Requests

- **Foreign Activity Inquiry**: Foreign Activity Inquiries are preliminary investigations of foreign national risks or threats to DHS and its components or other federal law enforcement or national security agencies that could impact U.S. National Security and are conducted and predicated on: 1) internal CISS security concerns or incidents; 2) support to law enforcement; 3) internal analytic projects targeting foreign trends, access, or anomalies of security concern; 4) incident reporting; and 5) Intelligence Community, law enforcement, or media reporting.
    - Foreign Activity Inquiries are assigned a case number and the Supervisor assigns the case to a Case Officer who then creates a Report of Inquiry.[4] A Case Officer conducts an inquiry using one or more of the below-listed Inquiry Activities to identify, validate, and/or corroborate evidence of security violations, criminal activity, terrorism

[3] Classified CISS requests (Requests for Information and Requests for Support) are entered into J-TIMS for tracking purposes only. Only minimal information such as the date of request, requestor, contact information, priority level, and a reference to on which classification network the request resides. The work for the Request for Information or Request for Support will reside on the respective classified network and will not be completed in J-TIMS.

[4] A CISS OPs Report of Inquiry is a preliminary investigative format used to determine if a full investigation is warranted or is in support of an investigation, in contrast to a Report of Investigation (also ROI), which serves as the standard format to report completed administrative or criminal investigations.

associations, foreign intelligence, foreign influence/targeting, and/or fraud associated with foreign nationals, foreign entities, and/or foreign governments. Evidence or associated documents are password protected and sourced in the Report of Inquiry as Exhibits. A Supervisor reviews and approves the case closure, and then furnishes the case to the CISS Director for concurrence prior to release or distribution. The Case Officer will document the final case closeout within J-TIMS following the acquisition or notification of a Disposition.[5] Per the National Archives and Records Administration (NARA)-approved retention schedules N1-563-09-1 and N1-563-08-4-2, CISS will retain information collected on foreign nationals, which is password protected, in Report of Inquiries and case files (exhibits, source documents) for twenty (20) years and cut off is at the end of the fiscal year of case closure. Longer retention is authorized if required for business use.

- Inquiry Activities:
  - Database checks (a list of systems used to conduct database checks is furnished below)
  - Documents or records reviews/examinations
  - Requests for DHS or external information or support
  - Comprehensive analysis (e.g., foreign travel)
  - Overt field operations, in coordination with DHS Headquarters or components, or other federal, state, local, and tribal agencies (e.g., operational security inspection, TechOps security scans)

- During the course of a Foreign Activity Inquiry, when security risks or threats are identified, they are referred to the OCSO Investigations and Operations Division, DHS Office of Inspector General, OCSO Insider Threat Division, Component Offices of Professional Responsibility, or other appropriate U.S. Government agency. Internal CISS Foreign Activity Inquiries are also conducted to support or enhance CISS policy and programs; discover, analyze, and mitigate foreign, operational security, and technical risks or threats; perform trend or statistical risk analysis; and protect DHS personnel, facilities, sensitive or DHS funded information and programs, IT systems and networks from foreign adversaries who seek to recruit, elicit, infiltrate, acquire access, steal, and/or do harm to the Department or U.S. National Security.
- Foreign Activity Inquiries may warrant broader notifications to U.S. Government

[5] A Disposition is referred to as the final case closeout within J-TIMS highlighting customer feedback or support results, which bears no time limit to acquire, but is evaluated to enhance customer service or to notify leadership of significant support, whereas the case closure depicts the actual date the request was fulfilled/completed.

agencies, including the Intelligence Community via an Information Intelligence Report or other reporting format. CISS Reports of Inquiry will not be shared or disclosed in an Information Intelligence Report or other reporting format to the Intelligence Community; however, foreign risk or threat related information is authorized for reporting purposes.

- Investigative support to law enforcement: Inquiries in support of an investigation of known or alleged fraud and abuse, and irregularities and violations of laws and regulations. Investigations are related to DHS personnel and programs administered or financed by DHS, including contractors and others having a relationship with DHS. NARA approved records schedules N1-563-08-4-2 and N1-563-09-1 applies to CISS OPs case files.
    - As with Foreign Activity Inquiries, cut off is at the end of the fiscal year in which the case is closed. Password protected Reports of Inquiry and case files (exhibits, source documents) are destroyed twenty (20) years after cut off. Longer retention is authorized if required for business use.

- **Requests for Information**: A Request for Information is a request for CISS "information," including information or an analysis of information derived from DHS and external databases not readily available to the requestor. The Request for Information is received via official U.S. government email or from the OCSO/Case Support Team via J-TIMS, then entered into the J-TIMS CISS Module, given a case number, and approved and assigned to a Case Officer by a Supervisor.
    - A Case Officer will query CISS holdings within the Integrated Security Management System (ISMS)[6] or via the databases listed below to acquire the requested information. If no records are found, or the information cannot be shared, the negative result is communicated back to the requestor by phone or email. Positive Request for Information results are highlighted in a password protected CISS memorandum, attached with the password protected source documents or referencing the location of any classified attachments, approved by the Supervisor, and returned to the requestor. Once received by the requestor, the Request for Information case is closed, but remains pending for a final disposition for case closeout in J-TIMS. Source documents are destroyed ninety (90) days from the date of closure, but longer retention is authorized if required for business use.

- **Requests for Support**: A Request for Support is a request for CISS "non-information,"

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

which involves some form of subject matter expert physical (hands-on) support. Requests for Support can include requests for CISS to furnish foreign adversary risk or threat briefings, conduct interviews or security audits, or inspect foreign gifts.

- The Request for Support validation and case creation process within J-TIMS follows the same procedures as a Request for Information; however, the approving Supervisor will send a courtesy notification to the CISS Director.
- Once the Request for Support is completed, the Case Officer will notify the Supervisor of the case status and results, follow up with the requestor to document a disposition and/or feedback based on provided OPs support, and then close the case. The CISS Director will be notified of the results of significant support requests.
- Requests for Support do not contain personally identifiable information.
- Request for Support records and supporting documents are destroyed twenty (20) years after support is completed, but longer retention is authorized if required for business use.

Privacy Impact Analysis

Authorities and Other Requirements

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

- 40 U.S.C. § 11331;
- Economy Act of 1932, as amended;
- Counterintelligence Enhancement Act of 2002;
- Intelligence Reform and Terrorism Prevention Act;
- Executive Order 12977;
- Executive Order 13286;
- Presidential Policy Directive/PPD-21, “Critical Infrastructure Security and Resilience” (February 12, 2013);
- DCI Directive 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)” (July 2, 1998); and
- Presidential Decision Directive (PDD)/NSC- 12, “Security Awareness and Reporting of Foreign Contacts” (August 5, 1993).

The System of Records Notices (SORN) that apply to CISS activities include:

- DHS/ALL-039 Foreign Access Management Systems,[7] which covers all records and information used by CISS related to the management and operation of DHS programs to safeguard DHS resources and information assets; and
- DHS/ALL-023 Personnel Security Management,[8] which covers records obtained by OCSO for personnel security responsibilities.

CISS safeguards records according to applicable rules and policies, including all applicable DHS databases' security and access policies. In accordance with NARA-approved retention schedules N1-563-09-1-1 and N1-563-08-4-2, CISS retains information in password protected Reports of Inquiry and case files (exhibits, source documents) for twenty (20) years, which are destroyed (20) years after a cut off at the end of the fiscal year in which the case is closed. Requests for Information supporting documents are destroyed ninety (90) days after case closure, but longer retention is authorized for business use.

Characterization of the Information

CISS OPs Review Process:

CISS OPs researches and analyzes information on foreign risks or threats using a variety of databases (listed below). CISS OPs collects personally identifiable information from foreign nationals and foreign entities requesting access to DHS, foreign sponsors, DHS employees and contractors sponsoring foreign access or with foreign associations, reported security incidents, employee reporting requirements, information in support of criminal or administrative investigations strategic foreign targeting projects based on foreign incidents/events, operational security, security audits and inspections, Requests for Information, Requests for Support, or Technical Operations trends, incidents, or concerns. To conduct this mission, CISS OPs creates Foreign National Personas (i.e., records on foreign nationals who are part of an OPs Inquiry or Request for Information), in the same manner outlined in the original J-TIMS Privacy Impact Assessment.[9]

Foreign National Persona (Subject, Co-Subject):

- Case Handle

[7] *See* DHS/ALL-039 Foreign Access Management, System of Records Notice, 83 Fed. Reg. 19078 (May 31, 2018), *available at* https://www.dhs.gov/system-records-notices-sorns.
[8] *See* DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 Fed. Reg. 8088 (February 23, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.
[9] *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.

- First Name
- Last Name
- Gender
- Date of birth
- Country of residence
- Country of citizenship
- Phone number(s)
- Email address(es)
- Company/Organization
- Position Title

Foreign National Associated Identification:

- Identification Type (Passport, Visa, Driver's License, Miscellaneous)
- Identification Number
- Identification Country
- Date Issued
- Expiration Date

CISS Requests:

- Request Number
- Request Status
- Request Type (Foreign Activity Inquiry, Request for Support, Request for Information)
- Classification
- Reported Event
- Inquiry Details:
    - Entity Type (Individual, Group, Miscellaneous)
    - Inquiry Type
    - Inquiry Category

- Request Details:
  - Priority
  - Foreign Country of Concern
  - Predication
  - Description
- Requester Information
  - Origin (Internal DHS or External DHS)
  - Requested By
  - Phone Number
  - Email
  - Agency
  - Component
  - Program Affected
  - Case Reference
  - OGC Representative
- Foreign National Information (associated with request)
  - Foreign National Subject
  - Citizenship
  - Position Title
  - Company/Organization
- Foreign National Visit Information
  - Visit Status
  - Visit Type Name
  - Visit Start
  - Visit End
  - Facility ID
  - Facility Organization Name

Foreign Activity **Inquiry:**

- Case Number
- Case Status
- Date Opened/Closed
- Priority level (routine, priority, urgent)
- CISS Request
- Supervisor
- Case Officer
- Predication
- Details
- Foreign Country
- Foreign National Subject (Foreign National Persona in J-TIMS)
- Non-Individual Name
- Result (Positive/Negative)[10]
- Disposition
- Date Initiated
- Date of Request
- Completion Date
- Exhibits (evidence, source documents)
- Law Enforcement support cases
    - Name of law enforcement official
    - Agency, Component, Office
    - Contact phone
    - Case number

Request for Information:

[10] "Positive result" means an inquiry has found derogatory information (i.e., security violations, foreign targeting of DHS, suspicious activity, criminal, fraud, or foreign terrorism associations/activity), validated source information, or acquired evidence of crime. "Negative result" means no information was found or source information was uncorroborated (i.e., "case closed").

- Case Number
- Priority level (routine, priority, urgent)
- Case Status
- Case Officer
- Predication
- Foreign Country
- Foreign National Subject (Foreign National Persona in J-TIMS)
- Result (Positive/Negative)
    - Positive results are furnished in a Memorandum
- Disposition
    - If classified, indicate where this information resides
- Date Initiated
- Date of Request
- Completion Date

Request for Support:

- Case Number
- Priority level (routine, priority, urgent)
- Case Status
- Case Officer
- Predication
- Disposition
    - If classified, indicate where this information resides
- Date Initiated
- Date of Request
- Completion Date
- Significant support or feedback is furnished in a memorandum to OCSO leadership

CISS OPs reviews and analyzes information from a variety of sources to which it has system access to furnish responses to requests, such as:

Internal

- U.S. Customs and Border Protection (CBP) Analytical Framework for Intelligence (AFI)[11]
- Integrated Security Management System[12]
- CBP Arrival and Departure Information System (ADIS)[13]
- CBP Automated Targeting System (ATS)[14]
- CBP TECS[15]
- U.S. Immigration and Customs Enforcement (ICE) Student and Exchange Visitor Information System (SEVIS)[16]
- Office of Biometric Identity Management (OBIM) Automated Biometric Identification System[17]
- U.S. Citizenship and Immigration Services (USCIS) Person Centric Query Services (PCQS)[18]

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ANALYTICAL FRAMEWORK FOR INTELLIGENCE (AFI), DHS/CBP/PIA-010 (2012 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF THE CHIEF SECURITY OFFICER, PRIVACY IMPACT ASSESSMENT FOR THE INTEGRATED SECURITY MANAGEMENT SYSTEM (ISMS), DHS/ALL/PIA-038 (2011 and subsequent updates), *available at* https://www.dhs.gov/publication/dhsallpia-038b-integrated-security-management-system-isms

[13] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ARRIVAL AND DEPARTURE INFORMATION SYSTEM (ADIS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-024 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR TECS, DHS/CBP/PIA-009 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM (SEVIS), DHS/ICE/PIA-001 (2020), *available at* https://www.dhs.gov/privacy-documents-ice.

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM, DHS/OBIM/PIA-001 (2012), and its successor system, HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY

External

- Department of Stat Consular Consolidated Database (CCD)[19]
- Department of Treasury Financial Crimes Enforcement Network (FinCEN)[20]
- Various Intelligence Community sources via classified networks
- Publicly available websites used to validate identities, addresses, contact information, and business data
- Commercial data sources, such as Lexis Nexis, Accurint, Thomson Reuters CLEAR, used to develop background information and to validate identities, addresses, associates, contact information, criminal records, and business data

CISS personnel always must corroborate accuracy of data through two or more sources. For example, J-TIMS is dependent on the Integrated Security Management System, the DHS authoritative source for DHS personnel security records to accurately populate persona information. Information is validated by CISS OPs Case Officers using multiple internal DHS and external DHS sources. Except for the use of the Integrated Security Management System to populate persona data (when available), there are no other system-to-system connections with J-TIMS. Any other data used by CISS OPs is data from internal DHS and other federal agency databases or requestors, checks of commercial or publicly available databases and websites, or information gathered during research or upon intake, and is manually entered into the system by CISS OPs Case Officers. Information not validated by an additional source is labeled as "uncorroborated" based on a single source. J-TIMS users are required by policy to alert data owners if records in an underlying system of record are identified as inaccurate and correct or delete the inaccurate data from J-TIMS.

Privacy Risk: There is a risk that information manually entered into the CISS Module may be inaccurate and that users may use the inaccurate information.

Mitigation: This risk is partially mitigated. Much of the information CISS OPs uses is from outside source systems and manually entered into J-TIMS. However, CISS OPs' standard operating procedures require Case Officers to confirm and validate identity using multiple sources. Information on Foreign National Personas derived from the Integrated Security Management System may contain inaccurate, unverified, or outdated information that is furnished by the foreign

IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE (PCQS), DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

[19] *See* U.S. DEPARTMENT OF STATE, PRIVACY IMPACT ASSESSMENT FOR THE CONSULAR CONSOLIDATED DATABASE (CCD) (2015), *available at* https://2009-2017.state.gov/documents/organization/242316.pdf.

[20] *See* U.S. DEPARTMENT OF TREASURY, PRIVACY IMPACT ASSESSMENT FOR THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN) (2015), *available at* https://www.fincen.gov/sites/default/files/shared/FinCEN_DCSD_PIA.pdf.

national and entered in the Integrated Security Management System by a DHS Security Official outside of CISS. CISS OPs Case Officers make every effort to validate an individual's identity, and correct inaccurate information derived from the Integrated Security Management System as necessary. Identities based on single source information, such as in an incident report, that cannot be verified are annotated as such in case files. Information that is manually entered into J-TIMS by CISS OPs users is peer-reviewed by a team lead or supervisor before being finalized and included in any referral or formal reports. PII is only shared with individuals with a need-to-know the personal information and is redacted from reports if, for example, it is shared as an "FYI"/for awareness purposes or with individuals without a need-to-know the specific PII. 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 the CISS Module is collecting more information than necessary for CISS OPs to fulfill its responsibilities.

Mitigation: This risk is mitigated. OCSO uses the minimal amount of information required to conduct case management through J-TIMS. This includes limiting the data imported from the Integrated Security Management System and data added manually. Additionally, CISS OPs personnel are trained on the sensitivity of the inquiry and investigative techniques, information, support, and records.

Uses of the Information

The information collected in the CISS Module is used to plan and direct requests for CISS OPs support, conduct inquiry and support activities (described above), process and analyze the information, produce a Report of Inquiry, furnish additional support or collaboration, and evaluate results, dispositions, and feedback to enhance policy and risk mitigation.

Privacy Risk: There is a risk that CISS Module users will access or 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 records and information in the system, as well as restrictions on disclosure mandated by the Privacy Act. Data entered into J-TIMS requires peer and supervisor review in accordance with the specific CISS Module standard operating procedure. Access to and actions taken by J-TIMS users are automatically recorded in the system's audit log and auditable in accordance with the CISS Module standard operating procedure.

Further, J-TIMS is a role-based system, limiting access to information based on the set permissions to the specific user role. The CISS Module has a designated owner who submits user account requests to J-TIMS system administrators for account provisioning. J-TIMS users do not have access to a module or information within a module unless they have an established need to know and their access is approved by the module owner and an administrator.

Notice

This Privacy Impact Assessment, as well as the System of Records Notices highlighted above, provide public notice of the collection, use, and maintenance of information in J-TIMS. Because J-TIMS is an investigatory case management system that collects and maintains sensitive information related to security, criminal matters, or investigations, it is not always feasible or advisable to provide notice to individuals at the time their information is input into the system. When CISS OPs Case Officers interact with individuals in connection with an inquiry, those individuals are generally aware that their information is being validated, recorded, and stored.

Privacy Risk: Given that CISS OPs acquires its data from other source systems, there is a risk that individuals will not know that J-TIMS maintains their data.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and the associated System of Records Notices provide a measure of transparency. However, because CISS OPs largely relies on data from other sources, J-TIMS information collection does not involve direct consent from the individual. CISS OPs relies on the source system to provide notice that the U.S. Government is maintaining their data.

Data Retention by the Project

CISS safeguards records according to applicable rules and policies, including all applicable DHS systems' security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing CISS records is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. In accordance with NARA-approved retention schedules N1-563-09-1 and N1-563-08-4-2, CISS retains information in password protected Reports of Inquiry and case files (exhibits, source documents) for twenty (20) years and cut off is at the end of the fiscal year of case closure. Longer retention may be authorized for business use. Request for Information attachments are destroyed ninety 90 days after case closure, but longer retention is authorized for business use.

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

Mitigation: This risk is mitigated. The CISS Module will retain Reports of Inquiry and case files (exhibits, source documents) for (20) years in accordance with NARA-approved retention schedules N1-563-08-4-2 and N1-563-09-1. CISS OPs will perform manual annual reviews in accordance with its standard operating procedures to ensure records are removed appropriately.

Information Sharing

Outside offices and agencies do not have access to the CISS Module in J-TIMS. Personally identifiable information is not generally shared outside of DHS as part of normal CISS OPs operations. However, when information may be shared on a case-by-case, need-to-know basis, it is done through official U.S. government email and is password protected, orally during briefings, interviews, official requests, and by telephone with other government entities, including law enforcement agencies and third parties with a need-to-know, in existing processes outside of J-TIMS. Further, as noted above, PII is redacted if the individual with whom the document is shared does not have a need-to-know the specific PII. The actual information shared depends on the nature, subject, status, and other factors unique to each investigation or information request. Any disclosures are annotated in the J-TIMS record.

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

Mitigation: This risk is mitigated. CISS OPs information is only shared with recipients within and outside DHS when sharing is aligned with the purpose for which the information was originally collected. Internal/external sharing is governed by DHS Directive 262-5 Information Sharing and Safeguarding and the DHS/ALL-039 Foreign Access Management Systems and DHS/ALL-023 Personnel Security Management System of Records Notices, which define the purpose for which the information was collected, and with whom and under what circumstances the information can be shared.

CISS OPs information is properly classified with special handling instructions and is password protected. Reports of Inquiry are marked For Official Use Only, Law Enforcement Sensitive. Reports containing Bank Secrecy Act or personally identifying information include a statement that information is not to be released to individuals who do not have a valid need-to-know without authorization from CISS.

The CISS Module also requires the Case Officer to acquire a disposition and feedback from the receiving agency. Users further receive annual training addressing the safeguarding of information through IT security and integrity awareness, as well as privacy awareness. CISS does not share information with entities other than the requestor without the requester's authorization. However, with approval by the CISS Director and OPs Supervisor, CISS may share non-attributed risk or threat information derived from Reports of Inquiry for other purposes such as operational security (i.e., training, awareness, foreign visit briefing/debriefing). Finished products such as security risk assessments are authorized for release to federal, state, local, and tribal agencies with the approval of the Chief Security Officer.

Redress

Because J-TIMS may contain sensitive information, DHS has exempted certain records maintained within the system from access. However, an individual may seek access to their records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or JRA still may seek access to records consistent with the Freedom of Information Act. Responsive records will be processed for release 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 Freedom of Information Act request to view their record(s), they may mail the request 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

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.

Auditing and Accountability

CISS Module users are security, intelligence, counterintelligence, and/or law enforcement trained. All personnel receive a copy of the CISS OPs standard operating procedures and on-the-job training; adhere to applicable policies, guidance, and procedures; receive training and testing from the J-TIMS program management team; complete mandatory annual online privacy training; and are provided a copy of this Privacy Impact Assessment.

Through the development of the CISS Module, three types of users were assigned roles within J-TIMS: Case Officer, CISS OPs Supervisor, and CISS Director. CISS OPs Supervisor and CISS Director are the J-TIMS Administrator with complete access and oversight. The Case Officer has access to view, create, and submit open requests and internal events. The CISS OPs Supervisor reviews, approves/rejects, opens, and assigns Foreign Activity Inquiry, Request for Information, or Request for Support cases. Once a case is approved, opened, and assigned by the CISS OPs Supervisor, the Case Officer conducts the case activity and ensures associated documents are properly classified with handling instructions (e.g., Unclassified//For Official Use Only). The

CISS OPs Supervisor reviews the case for closure, informing the CISS Director on a case-by-case basis, as appropriate.

Contact Official

William DeArcangelis
CISS Operations
Office of the Chief Security Officer
U.S. Department of Homeland Security
(202) 384-3929

Responsible Official

Thaddeus Bennett
Acting Director/Center for International Safety and Security
Office of the Chief Security Officer
U.S. Department of Homeland Security

Approval Signature

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

____

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