Privacy Impact Assessment
for the

Training Management Support System (TMSS)

DHS/ICE/PIA-053

May 5, 2020

Contact Point
James Malcolm
Section Chief, Accreditation and Training Systems
Office of Leadership and Career Development
Management and Administration
Immigration and Customs Enforcement
(202) 732-3335

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

Abstract

The U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) provides instructor-led in-residence law enforcement and career development training through its ICE Academies. ICE uses the Training Management and Support System (TMSS) to automate the administration and management of these training operations, including managing and tracking classes, registration, scheduling, training, testing, certifications, performance and conduct evaluations, Federal Law Enforcement Training Accreditation, and documentation. ICE is publishing this PIA because TMSS collects, uses, and retains personally identifiable information (PII) about ICE personnel (employees and contractors), employees from other Federal Government Agencies, and members of the public.

Overview

The development of a well-trained workforce is essential to ICE's success as a federal law enforcement agency in meeting its mission to protect America and uphold public safety by identifying criminal activities and eliminating vulnerabilities that pose a threat to our nation's borders, as well as enforcing economic, transportation, and infrastructure security. ICE uses its training academies to develop a well-trained workforce, provide comprehensive training that meets the needs of a wide variety of skillsets, promote innovative law enforcement techniques and equipment, enhance leadership abilities, and foster career development opportunities for both law enforcement and non-law enforcement personnel. Law enforcement personnel may take basic and advanced law enforcement training, and leadership and career development training is available to both law enforcement and non-law enforcement personnel.

TMSS supports all ICE Academies' instructor-led in-residence law enforcement and career development training. TMSS is a Commercial off the Shelf application consisting of a core training management system with eight functional areas: Testing, Registration, Scheduling, Performance Evaluations, Documents, Portal Framework, Portal Registration, and Personnel Portal. These functions automate law enforcement and career development training operations. TMSS provides lifelong training and certification records that are accurate, comprehensive, and legally defensible.

The ICE Office of Leadership and Career Development (OLCD) manages and uses TMSS. There are five other ICE program offices that also use TMSS:

- Enforcement and Removal Operations (ERO);
- Homeland Security Investigations (HSI);
- Office of Firearms and Tactical Programs (OFTP);
- Office of the Principal Legal Advisor (OPLA); and

- Office of Professional Responsibility (OPR).

Each program's specific use of TMSS is outlined below in Section 3.

TMSS Subjects and Typical Information

ICE students[1] consist of ICE employees, State and Local law enforcement officers as part of the ERO 287(g) program,[2] and foreign nationals as part of the HSI International Taskforce Agent Training (ITAT).[3] TMSS creates Person Records for all students; the bullets below give an example of the data that TMSS collects and stores in each Person Record for the law enforcement and career development training that TMSS tracks.

- Personnel, payroll, and employment data from the National Finance Center (NFC), ICE's payroll servicing agency, is collected for all ICE employees through an import;
- Biographical information, contact information, and other data is collected from law enforcement students during basic law enforcement courses;
- Test results (including the results of written exams);
- Class rosters;
- Student departure records;
- Student transcripts;
- Training history reports;
- Student records; and
- Instructor records, limited to contact information, certifications, and qualifications.

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?

Title 5, U.S.C., Chapter 41, Training; Title 5, C.F.R., Part 410, Training; Executive Order 11348, Providing for the Further Training of Government Employees, (Apr. 20, 1967).

[1] For the purpose of this PIA, the term "student" or "ICE student" will refer to ICE employees, individuals involved in ICE task forces, and state and local law enforcement operating under the ICE 287(g) program.
[2] For information about the ERO 287(g) program, see DHS/ICE/PIA-014 287(g) Program Database 2009.
[3] HSI International Taskforce Agent Training provides basic ICE-specific law enforcement courses to HSI Taskforce Agents to ensure that all HSI-led taskforces operate cohesively. Foreign taskforce agents are for the purposes of this document considered to be DHS Employees for the duration of their assignment.

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

TMSS collects information from ICE employees as well as members of the 287(g) program and task force members involved in the training. Emergency contact information may contain information from other members of the public (i.e., students' family members). TMSS information is covered by the following System of Record Notices (SORNs):

- DHS/ALL-003 General Training Records SORN,[4] which outlines the collection of information related to training DHS employees, federal employees, and volunteers.
- OPM/GOVT-1 General Personnel Records,[5] which covers the collection of records contained in the Enterprise Human Resource and Central Personnel Data File, including gender, race/ethnicity, and other personnel information.
- DHS/ALL-039 Foreign Access Management System of Records,[6] which covers the collection of passport numbers to allow access onto DHS owned facilities and to access DHS IT systems, which is necessary for training Foreign Task Force Officers.
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System,[7] which discusses the collection of identity information, including PIV credentials and identity documentation, to allow access to DHS facilities and IT systems.
- DHS/ALL-014 Personnel Emergency Contact Information System of Records,[8] which covers the collection of emergency contact information from students.

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

Yes, a system security plan was completed for TMSS. TMSS was enrolled in the ICE OCIO Information Assurance Division (IAD) Ongoing Authorization (OA) on 3/3/2013. Its most recent recertification was on 10/3/2018.

[4] DHS/ALL-003 DHS General Training Records, 73 FR 71656 (November 25, 2008).
[5] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[6] DHS/ALL-039 Foreign Access Management System of Records, 83 FR 19078 (May 1, 2018).
[7] DHS/ALL-026 DHS Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[8] DHS/ALL-014 DHS Personnel Contact Information, 83 FR 11780 (March 16, 2018).

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

ICE training records are maintained and disposed in accordance with National Archives and Records Administration DHS Records Schedule DAA-0567-2015-0009.[9]

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.

Personal information contained in TMSS is not covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

Categories of individuals about whom information is collected include DHS employees and members of the public. The following types of information are collected, generated, retained, accessible in, or disseminated by TMSS:

ICE Student Information (i.e., Student, Instructor, and TMSS User Records)

- Identifying Data: Name, Social Security number (SSN), Date of Birth (DOB);
- Race and Gender (for statistical purposes only);
- Employment Data: Duty Locations and Codes, Agency Entry on Duty (EOD) Date, Current Employment Status, Law Enforcement Indicator (Yes/No), Employing Organization Code, Position Title, Pay Plan, Grade, Step, Supervisory Code (Yes/No), ICE Network Login Information (user ID, password);
- Contact Information: Phone Number, Email Address, Home Address with Street, City, State, Zip Code; Mailing Address with Street, City, State, Zip Code;
- Personal Identifiers: Driver's License Number, Passport Number (for foreign students only), Visa Number (for foreign students only);
- Physical Indicators: Height, Weight, Eye Color, Hair Color;
- Health Information: Blood Type;

[9] *See* DHS Records Schedule DAA-0567-2015-0009 at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/daa-0567-2015-0009_sf115.pdf.

- Educational Data: Highest Level of Education, Degree Type and Year, Field of Study, Foreign Language Proficiency, Training Certifications for Students and Instructors; and
- Military Experience: Years of Active Military Experience, Branch of Military, Active Reserves/National Guard.

Information about Members of the Public

- Emergency Contact Data: Full Name, Mailing Address, Phone Number, Relationship to Student.

Information Disseminated from TMSS

- ICE's Training Reporting Repository (TRR) runs a nightly query to check TMSS for student graduations; if there are graduations, it creates a report listing student name, SSN, the program, class, and date of graduation, and imports the report back into TRR.

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

Information collected in TMSS comes from four sources:

- Training Reporting Repository (TRR)[10][11]

ICE's Office of Human Capital (OHC) downloads payroll, employment, and personnel data for all ICE employees from the NFC and provides it to TRR biweekly. A TMSS System Administrator (SysAdmin) then imports the data into TMSS. TMSS imports data on all new employees and/or updates to any existing employee's payroll or personnel data. As noted in Section 2.1 above, TRR also runs a nightly query to check TMSS for student graduations and creates a report that is imported into TRR; the data provides TRR with up-to-date student graduation information for training transcripts. Students from the ERO 287(g) program, as well as foreign nationals participating in HSI-led task forces, are not present in TRR. This is the only direct connection between TMSS and any other system.

- DHS Information Training Program Biographical Questionnaire[12]

[10] TRR is a system that ingests training data about ICE employees and contractors and provides accurate and complete reports, provides employees with a comprehensive training transcript, supports reporting for mandatory training, responds to training audits and data calls, and supports internal personnel investigations that require training information. TRR covers both in-person as well as online trainings.
[11] Participants in the ERO 287(g) program are not paid by ICE, so they are not present in the TRR ingests. Their information is collected through the DHS Biographical Questionnaire during their participation in basic law enforcement courses. Their updated emergency contact information is collected for advanced courses.
[12] Foreign nationals participating in HSI-led task forces are not paid by ICE, so they are not present in the TRR ingests. They also are not present in the ICE Active Directory. They only have access to basic law enforcement

All students taking basic law enforcement training complete the Questionnaire at the beginning of each class. The Questionnaire provides personal data such as biographical information, personal identifiers, and physical indicators. The Questionnaire collects physical indicator data in case of a medical emergency and to track physical fitness requirements set by ICE. The Questionnaire collects race and gender are for statistical purposes to show compliance with Federal rules and guidelines regarding diversity. OLCD imports data from the completed Questionnaires directly into TMSS and returns the Questionnaires to the students' program office for recordkeeping purposes.

- ICE Active Directory

On a quarterly basis, the TMSS SysAdmin submits a request to the ICE Service Desk for a spreadsheet of all ICE personnel email addresses and employment data from the ICE Active Directory. Foreign nationals participating in HSI-led task forces are not in the ICE Active Directory. Participants in the ERO 287(g) program are provided with ICE email addresses, and so are present in the ICE Active Directory. The SysAdmin imports the data into TMSS. TMSS uses ICE personnel email addresses to send notifications to students regarding training, including registration, enrollment, scheduling, and online testing. ICE personnel email addresses are also used to send TMSS users notifications regarding the system including availability, maintenance, etc. The ICE personnel employment data is quality assurance to ensure accuracy in importing the data into TMSS.

- Students

All advanced law enforcement and career development training courses collect updated emergency contact information from students at the start of each class. Training technicians, instructors, or class coordinators input the updated data into TMSS. Instructors collect emergency contact information at the start of every training course to ensure that the information remains accurate.

Foreign nationals participating in HSI-led task forces must undergo a vetting process by their task force's program office. Throughout the vetting process, the foreign national reviews this information for accuracy. The authorized program office TMSS user will then input the information into TMSS.

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

TMSS does not use commercial or publicly available data.

courses. As such, their information is only collected through the DHS Biographical Questionnaire.

2.4 Discuss how accuracy of the data is ensured.

Personnel, payroll, and employment data

OHC is responsible for ensuring the accuracy of the data received and processed by the NFC. If OHC or NFC makes and/or identifies an error, then OHC or NFC will provide a correction in a future biweekly download. TMSS uses multiple pieces of identifying data to ensure the accuracy of an import; if a discrepancy is found, it will be flagged. Identifying information includes SSN and employment data. The TMSS SysAdmin will work to identify the correct data in the event of a discrepancy, and will notify the data subject of the inaccuracy and the need to contact OHC to make corrections.

DHS Information Training Program Biographical Questionnaire

Because the student provides his or her own information on the Questionnaire, it is deemed accurate. If a student in an active class has reason to believe that the information he or she provided was incorrect or entered incorrectly into TMSS, or seeks to change or update his or her information, he or she may submit a request during training to the training staff to review the record and correct, if necessary.

ICE personnel email addresses

ICE's Office of the Chief Information Officer (OCIO) is responsible for the accuracy of email addresses in the ICE Active Directory. If an email address in TMSS is used and found to be incorrect, the TMSS user will notify the employee, who will need to work with OCIO to correct the email address.

Emergency Contact Information

Because the student provides his or her information, it is deemed accurate. If a student in an active class has reason to believe that the information he or she provided was incorrect or entered incorrectly into TMSS, he or she may submit a request during training to the training staff to review the record and correct, if necessary.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the system could contain inaccurate information.

Mitigation: This risk is mitigated. TMSS is configured to collect information from multiple sources. First, personnel, payroll, and employment data are collected from TRR and the ICE Active Directory. TRR and the ICE Active Directory have mechanisms in place to ensure data accuracy, such as reviews and audits by system administrators. Because students in basic law enforcement training provide their own information on the Questionnaire, it is deemed accurate. Similarly, information collected directly from students such as updated emergency contact

information, as well as information collected during foreign national vetting, is considered accurate because it is collected from the individual. If there is any conflicting data between TRR, the ICE Active Directory, and the Questionnaire, TMSS automatically flags the information to the TMSS SysAdmin for review. The TMSS SysAdmin reviews the sources of conflicting information, and may contact the data subject if necessary, to identify the accurate data. If possible, the SysAdmin will correct the inaccurate information; if it is not possible to correct the data (i.e., data from TRR/NFC), the SysAdmin will notify the data subject of the inaccuracy and the need to contact the responsible office to make corrections.

Privacy Risk: There is a risk of data duplication, as a subset of data is being extracted from one system and being loaded into a different system.

Mitigation: This risk is mitigated. Only the necessary data fields/elements from the source systems are replicated in TMSS for reporting or other purposes. If there is any conflicting data between these sources, TMSS flags it to the TMSS SysAdmin for review. The TMSS SysAdmin reviews the sources of conflicting information and may contact the data subject if necessary to identify the accurate data. The SysAdmin will correct the inaccurate information or notify the data subject of the inaccuracy and the need to contact the responsible office to make corrections.

Privacy Risk: The collection of an SSN or other sensitive data element presents an increased risk of identity theft if that information is compromised.

Mitigation: This risk is mitigated. The system limits access to PII to only those users having a need for that information in the course of their assigned duties and responsibilities. Further, TMSS employs role-based user access to minimize the opportunity for unauthorized individuals to access the system or its information. SSN is currently used as a unique identifier by the NFC for all ICE personnel and by the Federal Law Enforcement Training Center (FLETC) for students. TMSS uses SSN as the unique identifier because there is no ICE policy dictating what other unique identifier should replace SSN. OLCD is currently attempting to find a less sensitive unique identifier to align with DHS guidance.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The ICE Academies provide comprehensive training to meet the needs of a wide variety of skillsets, promoting innovative law enforcement techniques and equipment, enhancing leadership abilities, and fostering career development opportunities, all of which increase the effectiveness of the ICE workforce while minimizing the risks inherent to law enforcement operations. TMSS provides training and certification records that are accurate and comprehensive. TMSS creates Person Records for all students that contain the law enforcement and career development training

that TMSS tracks. Social Security numbers are used as the primary unique identifier to ensure accuracy in Person Records.

ICE program offices use TMSS to administer, manage, and track instructor-led in-residence law enforcement and career development training. TMSS automates training operations, including managing classes, curriculums, registrations, scheduling, training, testing, certifications, performance and conduct evaluations, accreditation requirements, reports, analytical tools, and documentation. OPLA and OPR have additional uses beyond tracking law enforcement and career development training. OPLA may use information from TMSS in the course of a civil or criminal case for the purpose of showing complete or incomplete training as necessary. Similarly, OPR may use information from TMSS in the course of an OPR investigation into an ICE employee.

ICE retains emergency contact information in TMSS in the event that a student has a medical or health emergency during a course. ICE assumes that the emergency contact remains the same unless the student changes the contact for a future training course. The emergency contact information is used to communicate any medical or health emergency to the student's designated contact.

All information provided is used as a basis for maintaining and processing records while the student is in training and managing the overall ICE training system. Students receive a list of potential uses, including but not limited to program validation, program and course evaluation, testing, posting of grades, appropriate intra-agency memoranda, emergency or other notifications, and such other record-keeping functions as are necessary and relevant.

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.

TMSS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or anomaly.

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

No. Only ICE personnel have assigned roles and responsibilities within TMSS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that individuals will use the information in the system for purposes beyond what is described in this PIA.

Mitigation: This risk is mitigated. ICE mitigates this risk in a number of ways. First, only authorized users with a need-to-know have access to TMSS and the PII contained within. Access roles are designated based on the individual's position, which ensures that users are only granted access to information necessary to perform their official duties. Individuals cannot access the system without an account created by the TMSS SysAdmin. To create a user account, OLCD collects the ICE Network Login Information and contact information from the requested user. Because the system is only available via the ICE network, only ICE personnel with a verified need to know can access the system.

Second, audit logs are reviewed on a regular basis by both the Information System Security Officer (ISSO) and TMSS SysAdmin to detect unusual activity within the system (e.g., login times, number of logins attempts, failed login attempts, changes to records). This ensures that the system is being used appropriately.

Third, retention periods are in place so that users do not have access to information beyond the appropriate time frame.

Fourth, anyone who is found to have used the system in an unauthorized manner will be disciplined in accordance with ICE policy and/or federal law. Finally, only TMSS SysAdmins can access and change all fields in the system, as well as grant access to other users.

Section 4.0 Notice

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

Students in basic law enforcement training courses are required to fill out the Questionnaire at the beginning of the course. The Questionnaire contains a Privacy Act statement to provide notice to individuals prior to the collection of information. The Privacy Act statement explains ICE's legal authority to collect the information, the purpose of collection, how ICE may share the student's information (including the student's SSN), and the impact if students do not provide ICE with all necessary information.

Much of the information present in TMSS comes from other ICE information systems (e.g., TRR, the ICE Active Service Directory). Any notice about the collection of information in other systems is beyond the scope of this PIA. Because the Questionnaire is the only information collected directly from the student, it is the only source of information that provides students with notice.

Further notice is provided by the publication of this PIA and the corresponding system of records notices.

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

The Questionnaire itself communicates to basic law enforcement training students the effects of not providing the requested information. Failure to provide all necessary information could result in the student being terminated from the course. If the information that is withheld is essential to effectively maintaining the student's records, the student will be informed, and if the student still does not furnish the required information, then his/her attendance will be terminated. The student's employment with ICE may be terminated as well. Because the information is necessary to process the student's records, there is no other recourse if the student wishes to continue in the course.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals chosen as a student's emergency contact may not be aware that their information may be contained within the system.

Mitigation: This risk is partially mitigated. Emergency contacts do not fill out the Questionnaire and so may not be provided notice that the student is using them as an emergency contact. However, it is presumed that the student will inform the emergency contact that they are being listed. The publication of this PIA and the corresponding SORN(s) provide detailed descriptions of the individuals whose information is contained in the system, the data stored by the system, and how the information is used. Individuals who suspect that information about them is stored in the system may seek access to the information by following the procedures described in the Redress section.

Section 5.0 Data Retention by the project

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

Records documenting attendance or participation at ICE training activities, including training, are cut off at the end of the calendar year in which the course is offered. These records will be destroyed 40 years after the cutoff in accordance with DHS Records Schedule DAA-0567-2015-0009.

Records are retained to document that the ICE employee in question has received training. Records may be used to certify that the employee meets employment standards, may be used in civil or criminal court cases, or in other circumstances when necessary.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the information will not be properly disposed of or deleted at the end of the retention period.

Mitigation: This risk is mitigated. OLCD will ensure that the information in the system is destroyed or disposed of in accordance with the applicable records schedule. ICE officers and employees will provide certificates of destruction or other applicable documentation to the ICE Records Division indicating that the records in the system have been appropriately disposed of.

Section 6.0 Information Sharing

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.

No, TMSS does not regularly share or disclose information with any outside agency as part of normal agency operations.

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

N/A.

6.3 Does the project place limitations on re-dissemination?

N/A

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Information from TMSS is not disclosed outside of DHS or ICE.

6.5 Privacy Impact Analysis: Related to Information Sharing

Because ICE does not share information from TMSS outside the Department, it has not identified any risks pertaining to information sharing.

Section 7.0 Redress

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

DHS Employees

Each ICE program office that uses TMSS to administer, manage, and track instructor-led in-residence law enforcement and career development training has its own policies for having current employees request transcripts from the system. Once a request is made to the program office, an authorized program TMSS user will provide the transcript. The TMSS audit trail ensures that the information is not improperly accessed or provided.

Members of the Public and Former ICE Students

Individuals seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE Freedom of Information Act (FOIA) Officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536
http://www.ice.gov/foia/

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

As mentioned above, any inconsistencies between the various sources of information in TMSS are flagged for review. If the TRR/NFC and/or Active Directory data is incorrect, the TMSS SysAdmin will notify the data subject of the inaccuracy and the need to contact the responsible office to make corrections. If a student in an active class has reason to believe that the information he or she provided was incorrect or entered incorrectly into TMSS, he or she may submit a request during training to the program training staff to review the record and make appropriate corrections.

Members of the public or former DHS Employees who discover an inaccuracy or error may submit a request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy
Attn: Privacy Division
500 12th Street SW, Stop 5004
Washington, D.C. 20536
http://www.ice.gov/management-administration/privacy

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

This PIA and the SORNs listed in Question 1.2 serve as notification for individuals about procedures for correcting their information. Moreover, the information gathered from basic law enforcement training students in the Questionnaire, as well as the emergency contact information, is considered to be accurate as it is provided by the employees themselves.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will have a limited opportunity to access and correct their data in the system or may not know that they have the ability to access/correct the information.

Mitigation: This risk is partially mitigated. There is no additional notice given to employees or emergency contacts at the beginning of a course, with the exception of the Privacy Notice in the Questionnaire for students of basic law enforcement training. Students in career development courses are not given notice because their information is pulled from other systems. However, this PIA and SORNs for both TMSS and source systems that outline redress procedures are publicly available.

Additionally, if a student believes that there is incorrect information in their TMSS records, they may contact the program office responsible for their training and request a review of their information.

Section 8.0 Auditing and Accountability

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

TMSS follows all relevant ICE IT Systems security standard operating procedures (SOPs) to ensure the security and integrity of all data contained within. Access to the information in TMSS is granted through the assignment of roles based on the user's need-to-know. Access designation is granted in a way that users are given the least amount of rights/privileges (i.e., read/edit/add/delete) that will enable them to perform their required tasks. These security measures, along with TMSS user training, system auditing, and other system safeguards, mitigate privacy risks.

TMSS also has audit procedures in place to meet control, reporting, and retention period requirements for operational and management reports. Reports generated by TMSS include audit logs, security rights reports, and usage statistics reports. Sensitive activities covered by the audit trail include, but are not limited to password resets, profile changes, and administrative functions. Audit records contain the following:

- Time and date of access (or attempted access) and exit from TMSS;
- Identity of each user (TMSS ID, Username [if privileged user], & IRMNET ID) accessing or attempting to access the system;
- Identity of each device (IP address) accessing or attempting to access the system; and
- All records updated by a user.

Audit logs are reviewed by the TMSS ISSO and SysAdmins at least monthly to ensure user accountability and system integrity.

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

All ICE employees, including TMSS users, must complete annual mandatory DHS privacy, records management, and cybersecurity training. TMSS users with access to full, unredacted PII, as well as SysAdmins, must complete additional role-based training annually. This TMSS-specific training ensures that these users know how to use the system and how to safeguard the accuracy and integrity of information contained within.

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

Access to the information contained in TMSS is limited by the user's defined role. A user's role and data permissions access are determined based on the user's ICE Program Office, job title, location, duties, and what TMSS functions the user needs to complete his/her assigned work. An employee needing to gain access to TMSS must submit the *TMSS User Account Access Request* form. The employee submits a completed form, including a digital supervisory signature, through the ICE Service Desk, in accordance with the procedures in the *OLCD Standard Operating Procedure to Request Support or Help with the TMSS*. The TMSS Business Owner, who is the Program Manager overseeing TMSS, receives and reviews the form to ensure that the user will have access commensurate to his/her role(s) and duties, prior to giving approval. The TMSS Business Owner forwards approved forms to a TMSS SysAdmin for account creation. Guest or anonymous accounts are specifically disallowed. Temporary accounts are prohibited. Individuals without an account created by the SysAdmin cannot access the system. Anyone who is found to have used the system in an unauthorized manner will be disciplined in accordance with ICE policy and/or federal law.

All TMSS users are required to have an ICE Personal Identity Verification (PIV) card to access the system. TMSS users use an Active Directory username to support single sign-on (SSO). For login, SSO uses IRMNET authentication to validate the user. All access to TMSS is through Government Furnished Equipment (GFE). No users from other agencies have access to TMSS.

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?

TMSS information is not shared or disclosed as part of any information sharing agreements, and no information is accessible by organizations outside of ICE. If this changes in the future, ICE will publish a Privacy Impact Assessment Update to cover any changes.

Responsible Officials

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

[Original signed and on file with the DHS Privacy Office]

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security