Privacy Impact Assessment Update
for the

FPS Training and Academy Management System

DHS/CISA/PIA-024(a)

July 02, 2019

Contact Point
Eric L. Patterson
Director, Federal Protective Service
U.S. Department of Homeland Security
(202) 732-8000

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security's (DHS) Federal Protective Service (FPS) Office of Training and Professional Development (TPD) maintains a robust automated training and certification system called the Training and Academy Management System (TAMS). TAMS provides FPS TPD the ability to track, monitor, and verify training for federal law enforcement officers and security personnel. FPS is conducting this Privacy Impact Assessment (PIA) update because several new functionalities of TAMS involve the personally identifiable information (PII) of FPS personnel and contracted security personnel.

Overview

FPS TPD is responsible for ensuring that FPS law enforcement personnel are properly and effectively trained to execute their law enforcement duties. FPS TPD also conducts professional training and provides professional development opportunities for all FPS employees and Physical Security Officer (PSO) contractors to ensure they are well trained and nationally recognized as outstanding professionals and law enforcement security subject matter experts. FPS TPD uses TAMS to serve as a robust automated training and certification system.

TAMS collects and maintains information on FPS employees, contracted personnel, and employees of other federal agencies. The purpose of TAMS is to create and maintain training records that demonstrate the application of training policies and standards, as well as applicable law enforcement and professional certifications. TAMS manages the life-cycle of all learning activities for FPS law enforcement employees and contractors. TAMS serves as a gateway for FPS law enforcement personnel, students, instructors, supervisors, and administrators to access trainings that will provide them with the skills and knowledge necessary for effective and safe enforcement of the law and the conduct of daily operations. TAMS is the system of record that records, stores, and reports training records; reports and alerts training requirements and needs; provides test banks for classroom and online testing; provides the framework for Academy and course accreditation; provides the framework for training validation and evaluations; schedules students and instructors for classes; provides instructor development and certification; provides a training records validation and audit tool; administers, tracks, and validates FPS Field Training and Evaluation Program (FTEP) training; tracks K-9 Team basic training, refresher training, and certifications; and tracks career path development. TAMS will serve as a repository for records derived from field-based trainings, certifications, and the like, with records access restricted to system administrators to use for reporting and tracking purposes.

Person Record Initiation in TAMS:

TAMS receives bi-weekly data extract files from the FPS Employee Information System (EIS)[1] containing data from the U.S. Department of Agriculture's National Finance Center

[1] The Enterprise Information System (EIS) is a legacy FPS portal that hosts a number of FPS-specific applications in

(NFC),[2] used to populate federal FPS employees personnel records in TAMS.

Personnel records for contracted PSO Personnel are created in TAMS using several available data resources to include the DHS Office of the Chief Security Officer's Integrated Security Management System (ISMS)[3] and Identity Management System (IDMS)[4] data, and FPS Contract Management Tool (CMT)[5] data. Through cross-referencing of the various data sources, FPS is able to determine an accurate number of PSOs cleared to work on FPS contracts/sites. PSO data is imported from all three data sources on a bi-weekly basis. Importing the data is a manual, Excel spreadsheet-based process conducted by the TAMS Administrator and the TAMS Data Management Team.

TAMS also stores and tracks training for external students who serve as law enforcement officers at other federal, state, and local agencies. Profiles for external students are created by the TAMS Administrator. The information obtained, stored, and tracked for external students differs from that of the federal FPS employees and contractors, as TAMS will only collect external students' basic contact information.[6]

Information collected from external students:

- Full Name;
- Organization Name;
- City and State (of work location);
- Work Telephone Number;
- Work Email Address; and
- Type of Training Certification received.

Access to and use of TAMS:

Students do not readily access TAMS. TAMS was designed initially to assist TPD, regional training personnel, and other FPS administrative personnel to efficiently carry out their responsibilities (i.e., create and maintain training records; automate training administration functions; automate course assignments and schedules; process test results and grades; and manage reporting requirements). However, students are granted access to TAMS on an as-needed basis, to

a secure environment. These applications have been developed by the FPS Information Technology Division to capture data to support the mission of FPS, and to produce analysis and management reports based on this data.

[2] More information on the NFC is available at: https://www.nfc.usda.gov/.

[3] For information on ISMS, see DHS/ALL/PIA-038(b) PIA, *available at* www.dhs.gov/privacy.

[4] For information on PIV/IDMS, see DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System PIA, *available at* www.dhs.gov/privacy.

[5] CMT is a Microsoft Access database application designed to assist Contract Officer Representatives (COR). CORs perform several key contract management functions to include: Invoicing, Scheduling, Administrative Records Audits, Inspections, and tracking of training and certification data. CMT access is account/permissions based and accessible through an FPS-sponsored SharePoint site.

[6] This basic contact information generally consists of name, organizational information, work location, work contact information (e.g., phone, email address), and training certification information.

allow for self-registration for training courses, check training schedules for details related to an upcoming training course, or review training materials such as student guides and reading assignments. Students will access TAMS through the TAMS Portal to take online examinations, check reading assignments, check grades, and instructor communications during course participation. Once the course has been completed, and all requirements for the students to access TAMS have been completed, the student's access rights will be removed.

The TAMS Portal is accessed through Single Sign-On (SSO), which uses the DHS-issued Personal Identity Verification (PIV) card and the DHS Active Directory e-authentication functionality. For external students, TAMS student access will now be granted through the public-facing Homeland Security Information Network (HSIN) federal connection portal.[7]

Reason for the PIA Update

The TAMS PIA update is being submitted to discuss several new functionalities of TAMS that will involve the PII of FPS personnel, contracted security personnel, and external students.[8]

Data Interface with the DHS TIE for ISMS Data

TAMS will now interface with the DHS Trusted Information Exchange (TIE)[9] to receive personnel security data from ISMS related to FPS government employees and contracted PSO employees. By using the TIE to receive ISMS data it eliminates the FPS Personnel Security Division's need to manually import ISMS data into TAMS, improving accuracy and timeliness. TAMS data will not be transmitted back to the TIE because this is a one-way flow of information.

ISMS data contains the Electronic Data Interchange Personal Identifier (EDIPI)[10] that will be used to determine the identity of individual records that already exist in TAMS and will be used to create person records when new employee data is identified by TAMS. Data elements will include name; EDIPI; date of birth; clearance status; employing contract number; citizenship; position title; contract company name; pre-appointment date; final fitness date; and National Security Investigation (NSI) clearance date, and other related personnel data.

[7] For information on HSIN, see DHS/ALL/PIA-061-1 HSIN Release 3 user Accounts: HSIN Enterprise Reporting Solution PIA, *available at* www.dhs.gov/privacy. For more information on the HSIN functionality, see "Public-Facing Portal through HSIN" section below.

[8] External students referrers to those who do not have a government issued PIV card thus can only access TAMS via the HSIN public-facing portal.

[9] For information on the TIE, see DHS/ALL/PIA-050 DHS Trusted Identity Exchange PIA, *available at* www.dhs.gov/privacy.

[10] EDIPI is a unique 10-digit number associated with an employee's PIV card.

Public-Facing Portal through HSIN

TAMS will now use HSIN to facilitate use of the system for external students. HSIN will provide a federation and dual-factor authentication support to allow non-federal PSO personnel and other external students' access to the TAMS Portal to input training and certification data.

Permitting FPS's corporate partners to manage their own records is a critical component of the TAMS implementation strategy for two main reasons. First, the administrative burden associated with managing over 14,000 personnel records is beyond what can be managed with on-hand federal labor. Second, the most effective way to obtain current, reliable data is to source that data from its point of origination, the PSO vendor.[11] As most of the PSO community does not possess PIV cards to allow for SSO capabilities, the Director of FPS tasked the Innovation & Technology Division (ITD) with identifying a viable network access solution for FPS's PSO corporate partners and HSIN was determined to be the most efficient and secure access point available to FPS.

HSIN ensures the trust of its users through enhanced security measures, including verifying the identity of all users the first time they register, and ensuring they all use two-factor authentication each time they log on. HSIN leverages the trusted identity of its users to provide simplified access to the TAMS Portal. A TAMS Community of Interest (COI) has been established to track and maintain PSO and external student requests to gain access into the TAMS User Portal. The TAMS Program Manager will act as the TAMS COI administrator and will process all nomination applications for access into TAMS. Once accepted, nomination applications are forwarded to the HSIN TAMS Advocate for HSIN account processing. HSIN generates an email to the nominated applicant and he or she is prompted to complete and online profile that is used to verify the identity of the user. Once cleared the user receives a user name and password and is prompted to log into HSIN to complete the process by logging in and verifying his or her identity through HSIN's dual-factor authentication process. After the user successfully gains access through the HSIN authentication process, the individual is then sent to the TAMS COI page where he or she can access the TAMS Portal. Once the user gains access to the TAMS Portal, he or she will be able to enter and maintain training and certification data for the employees under his or her purview. Users will also be able to request and participate in training courses, manage personal contact information, view employment histories, and varying levels of organizational data.

TAMS Portal capabilities are role and permission based and are granted by the TAMS Administrator dependent on the tasks the user needs to complete in the system.

TAMS Mobile Application

FPS has developed a TAMS mobile application, which will allow for the use of issued government furnished equipment, specifically cell phones, to record the results of training events

[11] Vendor refers to FPS Corporate Partners; these companies provide the FPS contracted security personnel working in federal buildings nationwide.

and exercises while in the field or at remote training sites. The mobile application is used by instructor staff who have been granted specific permissions that allow for mobile entry. An approved and authorized instructor must first access the instructor portal and scan a system provided QR code to activate the mobile application on his or her mobile device before use. The instructor must also be granted the mobile grade entry status as part of a scheduled and approved class in TAMS, which allows him or her to access student rosters and approved testing materials. The mobile application will only be used by instructors or authorized field personnel to record test results, practical exercises, and field activities.

<u>Data Interface with FPS PTS</u>

FPS currently has a paper-intensive and time-consuming processing structure in place to manage PSOs who are assigned at various locations. The current PSO management process relies heavily on contractor self-reporting and is supported by technology (to the extent that the process is automated) that has significant capability gaps. Therefore, FPS has identified mission functions that must be executed to better manage its PSO program, such as:

- The ability to remotely confirm that guard posts are staffed as required;
- The ability to verify PSO certifications and suitability findings to ensure that FPS posts are staffed by qualified and cleared PSOs;
- The ability to automatically gather and store PSO Management data needed to validate contract invoices, respond to data calls, provide management reports, and analyze performance; and
- The ability to verify time and attendance of PSOs.

Post Tracking System (PTS) is a web-based application that will automate this paper intensive process and address current mission and capability gaps. TAMS will interface with PTS to facilitate the process of PSO certification and suitability verification.[12] This interface will automate the process by providing qualification data from TAMS to PTS depicting all the training and certifications a PSO has obtained. This qualification data will be used by PTS to determine if the PSO qualifications match the post requirements and if that individual is qualified. For example, if a location requires a PSO to be certified in Cardiopulmonary Resuscitation (CPR) and First Aid, PTS will use TAMS to verify that the PSO have met those requirements to be posted at that location.

The information exchange is only in one direction, from TAMS to PTS. The data extract from TAMS to send to PTS[13] will include the following for each PSO qualification:

[12] *See forthcoming* FPS PTS PIA *available at* www.dhs.gov/privacy.

[13] Currently, this extract is a manual process that occurs daily. The extract is sent in an encrypted spreadsheet via email from the TAMS system administrator to the PTS technical lead. The PTS technical lead then manually uploads the data into PTS.

- Full name;
- EDIPI;
- Citizenship;
- Contract Number, Contractor Company;
- Clearance Type, Condition, and Status;
- Qualification Type and Name; and
- Qualification Start (issued) and End Dates.

Privacy Impact Analysis

Authorities and Other Requirements

The same authorities from the previous TAMS PIA continue to apply and the same system of records notice (SORN) are still applicable.

Since publication of the previous TAMS PIA, the National Archives and Records Administration (NARA) has updated its General Records Schedule (GRS). GRS 2.6 Employee Training Records (Items 010 and 030) is now applicable to non-mission related training records. Mission-related training records are now maintained under DHS Records Disposition Authority N1-563-08-11.

Characterization of the Information

In addition to the interfaces and data collection efforts listed in the previous TAMS PIA, TAMS now interfaces with the DHS TIE for an automated import of ISMS data. However, no additional or new data elements will be received via ISMS other than those already identified in the original PIA.

TAMS will now use HSIN as an access point for external users. Through the HSIN registration process, new information may have to be collected from external users, but that information is not passed through to TAMS. External students will still be required to provide the same information outlined in the previous PIA to access TAMS.

The newly developed TAMS mobile application provides instructors the ability to record test results while in remote locations and away from a traditional classroom. Access to the TAMS mobile application is limited to authorized instructor staff assigned to classes that have tests (to record test results) or events (to record practical exercises and field activities) that can be tracked by the application. This functionality does not require TAMS to collect any new data elements; rather it provides a new way for information to be input into TAMS.

TAMS is sharing PSO vendor training and certification data with FPS PTS. This information sharing was previously done manually with the same data.

Data that is collected in TAMS continues to be used for the creation of person records and for the proper and effective tracking of training and certification requirements. The sources of data include IDMS, ISMS, the PSO Master Certification List,[14] NFC, and directly from the TAMS user community (made up of students, instructors, and system administrators).

FPS relies on the accuracy of employee data that is received from the data sources outlined above. Individuals may verify their information/record within TAMS for accuracy if they are granted access. Individuals may request corrections to their data by contacting their HR specialist for the correction of NFC data, the TAMS system administrator for TAMS-related personnel record data, or contracted personnel may contact their COR or the designated contractor POC for the submission of corrections. Additionally, the new functionalities within TAMS allow for greater accuracy because there are fewer manual transfers and entries of data and users will be able to modify non-critical information themselves.

Privacy Risk: There is a risk that a public-facing HSIN portal will allow unauthorized access to personal information.

Mitigation: This risk is mitigated. Only authorized PSO users will be granted access via HSIN. Vendors are provided with a dual-factor authentication methodology to update training records, confer certifications, and renew expiring certifications. PSO users will be identified by the vendor companies and will be nominated for TAMS HSIN accounts. The TAMS Program Manager will approve nominations and create HSIN accounts for the PSO users.

Uses of the Information

TAMS uses various data sources to ensure data accuracy for a variety of employee categories from government employee to contracted security officers. ISMS data from the DHS TIE interface contains data elements already in use in TAMS that had been previously manually imported from data files provided by the FPS Personnel Security Division.

The public-facing access point through HSIN allows authorized PSO vendor representatives the ability to enter and maintain training and certification data for their respective contracted security workforce. The data provided by the PSO vendor representatives is shared through to FPS PTS to determine if a PSO is properly trained and current on certifications that will allow him or her to stand a security post in a federal facility.

The TAMS mobile application has been developed to allow instructors the ability to enter student test and training data using their government-furnished mobile devices while observing training when away from a traditional classroom environment. Data entered into the mobile application is sent to TAMS, and the class and student records are updated with the pertinent information. Access to the mobile application is limited to authorized instructor staff assigned to classes that have tests or events that can be tracked by the mobile application.

Privacy Risk: There is a risk for misuse or mishandling of information by system users.

[14] The PSO Master Certification List is a report generated by the FPS Core Management Tool (CMT). CMT will be replaced by the more secure HSIN connection.

Mitigation: This risk is mitigated. All TAMS users have role and permission-based access granted by the TAMS system administrator based on the need to perform certain actions in the system. Roles and permissions-based access is granular in TAMS and can be modified to meet security challenges or identified access needs. Permission-based access helps prevent users from accessing information beyond their need-to-know. TAMS uses an audit log report that can be generated to track all system activities conducted by anyone who is granted access to the system at any level. All users must also sign the TAMS Rules of Behavior form before access is granted. Training is provided for specific functionalities within TAMS once permissions are assigned. Training must be completed before access is granted.

Notice

FPS continues to provide notice on the collection of personnel, contractor, and student information when individuals log into or access TAMS. Notice is also provided by way of a TAMS-approved Privacy Act (e)(3) Statement, SORNs applicable to this system, and through the publication of this PIA. Additionally, all users sign a TAMS Rules of Behavior form that is appended to their person record in TAMS when they become users. Each time the user logs in, he or she also must accept the privacy policy before proceeding.

Separately, HSIN provides notice to users regarding the expected user behaviors when registering for access to the system and then while accessing HSIN thereafter. Additionally, notice to TAMS mobile app users will be provided when the app is accessed.[15]

Data Retention by the Project

The National Archives and Records Administration (NARA) has updated its General Records Schedule since the previous TAMS PIA was completed in 2016. TAMS non-mission training records now follow the NARA GRS 2.6, *Employee Training Records*, Items 010 and 030. Mission-related training records now follow DHS Records Disposition Authority N1-563-08-11. In order to conform to these retention requirements, TAMS has been configured to automatically purge data in accordance with the NARA-approved retention schedule.

GRS 2.6 Item 10 files:

- Non-mission related items such as, correspondence, memoranda, agreements, authorizations, reports, requirement reviews, plans, and objectives relating to the establishment and operation of training courses and conferences will be destroyed when three (3) years old.
- Background and working files correspondence, memoranda, reports, and other records relating to the availability of training and employee participation in training

[15] Currently the TAMS mobile app is still in development and not operational. The app is mentioned in this PIA because operational status is expected within the life-cycle of this PIA update.

programs sponsored by other Government agencies or non-Government institutions will be destroyed when three (3) years old.

GRS 2.6 Item 30 files:

Certification files documenting attendance or participation at DHS-sponsored training activities such as training, seminars, attendance at conferences, office "lunch and learns," and special project assignments will cut off at the end of the calendar year in which the certification is received and will be destroyed when three (3) years old.

DHS Records Disposition Authority N1-563-08-11 files:

Mission-related training materials used for training in functions or activities related to goals of DHS and its programs to include training course plans, instructional materials, and other training aides will cut off at the end of the calendar year in which course or the material is superseded. Materials will be destroyed 30 years after cutoff.

Agency-sponsored routine training records including copies of manuals, syllabi, textbooks, and other training aides developed by the agency will cut off at the end of the calendar year in which course or the material is superseded. Course materials will be destroyed 10 years after cutoff.

Information Sharing

There are no changes to the Information Sharing since the 2016 TAMS PIA.

Redress

With the implementation of the HSIN external access portal, employees, contractors, and external students will have access to their individual person record in TAMS. Users will be able to modify non-critical information such as mailing address, contact phone numbers, and emergency contact information. Users will also be able to view their individual learning history, class documentation, career role progress, and employment history.

Auditing and Accountability

FPS uses technical controls to ensure that information is used in accordance with the stated practices in this PIA. FPS uses permission and role-based access controls to limit user's access to information. System users, specifically those who are employees or contractors to FPS, must have a valid and active DHS network account to access TAMS. External students are verified through the HSIN registration and identity solution process. TAMS also has full audit capability for all data changes in the system.

All FPS users that will access the system in an elevated capacity are required to complete DHS IT security awareness training. This training, along with a signed TAMS Rules of Behavior form are required for granting access to the system. These documents are then uploaded into TAMS on the user's person record as part of the system security compliance requirements.

Requests for access to TAMS as a user with elevated roles and responsibilities will come from the requestor's organization of record. The request form is an automated TAMS specific electronic form and is accessed and completed on the login page of the TAMS Portal. The requested user's information will be processed by the TAMS COI administrator. Once all clearance requirements are met and access has been established by HSIN, the user's TAMS Portal account will be created or activated if already in the system.

Any memoranda of understanding would be reviewed by the system owner, program manager, FPS Privacy Officer, FPS Office of the General Counsel, and then forwarded to DHS for formal review.

Responsible Official

Eric L. Patterson
Director, Federal Protective Service
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security