Privacy Impact Assessment
for the

FPS Training and Academy Management System

DHS/NPPD/PIA-024

August 25, 2016

<u>Contact Point</u>
Eric L. Patterson
Director, Federal Protective Service
National Protection and Programs Directorate
(202) 732-8000

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

Abstract

The National Protection and Programs Directorate (NPPD) Federal Protective Service (FPS) Training and Professional Development (TPD) division has acquired a robust automated training system called the Training and Academy Management System (TAMS). The goal of TAMS is to provide FPS TPD with tracking, monitoring, and verification of training for federal law enforcement and security personnel, and to empower them with the skills and knowledge necessary for effective and safe enforcement of the law. NPPD, FPS is conducting this Privacy Impact Assessment (PIA) because, once fully implemented, TAMS will collect, maintain, use, and disseminate personally identifiable information (PII) about individuals attending the FPS Academy.

Overview

The Department of Homeland Security's (DHS) National Protection and Programs Directorate's (NPPD) Federal Protective Service (FPS), Training and Professional Development (TPD) division is responsible for ensuring that all FPS team members are properly and effectively trained to execute their respective law enforcement duties. FPS TPD conducts state-of-the-art professional training and provides professional development opportunities for all FPS employees and Physical Security Officer (PSO) contractors in order to ensure they are well trained and nationally recognized as outstanding professionals and law enforcement security subject matter experts. FPS TPD has acquired the Training and Academy Management System (TAMS) to serve as a robust automated training tracking system.

TAMS collects and maintains information on FPS employees, contracted personnel, and employees of other federal agencies.[1] 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. Once fully deployed, TAMS will manage the life-cycle of all learning activities for FPS law enforcement employees and contractors. TAMS will serve as a gateway for FPS law enforcement personnel, students, instructors, supervisors, and administrators to access trainings that will empower them with the skills and knowledge necessary for effective and safe enforcement of the law. At its end state, TAMS will be a system that records, stores, and reports training records; reports and alerts training requirements and needs; provides test banks for classroom and on-line testing; provides the framework for Academy and course accreditation; provides the framework for training validation and evaluations (surveys); schedules students and instructors for classes; provides instructor development and certification; provides a

[1] *See* DHS Delegation Number 17001-01, Delegation to the Under Secretary for National Protection and Programs, Section II.W.6, dated October 25, 2013.

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 initially restricted to system administrators to use for tracking purposes.

Student Profile Initiation in TAMS:

TAMS will receive bi-weekly data extract files from the U.S. Department of Agriculture's National Finance Center (NFC) to pre-populate the necessary FPS employee data and create student profiles for those employees attending the FPS Academy. The NFC provides human resources and administrative services for many agencies of the United States Federal Government. Student profiles will also be initiated for FPS contractor employees; however, this will be a manual process completed by a TAMS system administrator. Contract program managers and designated contract training officers will provide the required data to the respective TAMS system administrator in order to create the student profiles for FPS contractors. This information is derived from contractor on-boarding and training documentation.

TAMS will also store and track trainings for external students who serve as law enforcement officials at other federal agencies. These students' profiles will be created manually by the respective TAMS system administrator; however, the information obtained, stored, and tracked for external students is different than that of the other categories of students, as TAMS will only collect external students' basic contact information. External student profiles will be created by a TAMS system administrator via a manual process.

Access to and use of TAMS:

Although student profiles will be created, students will not readily access TAMS. The system is initially being designed to help training staff, regional training personnel, and other administrative personnel more 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 can be granted access to TAMS on an as-needed basis, as this will allow students to self-register for training, check training schedules for details related to an upcoming training course, or review training materials such as a student guide. There are also specific online courses and exams that students will need to take that are only available in TAMS. Therefore, students will need access to TAMS in order to fulfill their training requirements, and pending future enhancements to the system, student access to TAMS will be controlled by way of a manual function of the system administrator. Once the student completes his or her online exam within TAMS, the system administrator will deactivate access permissions for the student. As TAMS is further built out in the future, additional capabilities will be available to the students. At that time, FPS employee and contract PSO students will have the ability to log into the TAMS user access portal using their respective Personal Identity Verification (PIV) card via Single Sign On (SSO), which uses DHS Active Directory e-authentication. For students from an agency outside of FPS, TAMS student access will be generated when a system administrator verifies the student's need to access TAMS and offers instructions for the student to log in. The instructions advise that the student shall log in using his or her username (the student's email address) and an assigned temporary password; which upon initial log in, the student is prompted to change. The future build out of TAMS will afford all students the capability to access and view upcoming training dates, locations, training requirements, and his or her record data.

In addition to the extensive test administration and tracking functions that will benefit regional training coordinators, FPS administrative personnel, supervisors, and management, TAMS will prove to be equally beneficial to the students. While students will initially only be provided with access to TAMS on an as-needed basis during certain times related to their online required trainings, field based trainings, and certifications, future TAMS capabilities will allow students to register for training courses, review and track their own training record data, and print certificates to provide to supervisors and management after the successful completion of training.

TAMS contains Certification Masters that once assigned to a student, will track when and what training has been accomplished to maintain certifications, as well as send notifications of training that is due to maintain certifications. Notification alerts are sent out to the students, through TAMS, to the supervisor, and to the regional training coordinator. Notification alerts begin 120 days prior to the expiration of a certification, and then at 30 days intervals until the training is completed or the certification has expired. If a student is in danger of failing a class based on recorded tests/exams or observed reports, a flag is appended to his or her student record that can be viewed by TPD staff and supervisors so that appropriate actions can be taken. In the event that the student fails a class/course, he or she is able to view his or her results and a notice is sent to his or her respective supervisor and regional training coordinator with information on the necessary next steps for remediation or dismissal. The message includes the information of a TPD point of contact for follow up as necessary.

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?

NPPD FPS is authorized to collect this information pursuant to:

- 5 U.S.C. § 4103 Establishment of training programs;

- 5 U.S.C. § 4302 Establishment of performance appraisal systems;
- 5 CFR Part 410, Training;
- 5 CFR Part 430, Performance Management;
- Executive Order 13111, Using Technology to Improve Training Technologies for Federal Government Employees;[2]
- Executive Order 11348, Providing for the Further Training of Government Employees;[3] and
- DHS Delegation Number 17001-01, Delegation to the Under Secretary for National Protection and Programs, Section II.W.6, dated October 25, 2013.

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

The collection of the PII maintained in TAMS is covered by the following SORNs:

- DHS/ALL-003 Department of Homeland Security General Training Records;[4]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[5]
- DHS/ALL-014 Department of Homeland Security Emergency Personnel Location Records System of Records;[6] and
- DHS/ALL-025 Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security.[7]

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

The Certification & Accreditation for TAMS has an anticipated completion of late August 2016, and the TAMS ATO is expected to be granted in August 2016.

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

Yes. The training records in TAMS will follow the General Records Schedule 1, item 29, Training Records.

[2] Exec. Order No. 13111, *reprinted as amended* in 5 U.S.C §4103 note.

[3] Exec. Order No. 11348, *reprinted as amended* in 5 U.S.C §4103 note.

[4] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (Nov. 25, 2008).

[5] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).

[6] DHS/ALL-014 Personnel Emergency Contact Information, 81 FR 48832 (July 26, 2016).

[7] DHS/ALL-025 Department of Homeland Security Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security, 75 FR 5614 (Feb. 3, 2010).

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.

There are no formal information collections associated with this system. Information is collected by way of the NFC, the Contracting Officer Representative (COR), and directly from the student.

Section 2.0 Characterization of the Information

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

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

There are two different categories of individuals for whom the information is collected:

1. FPS employees and contractors; and
2. Employees of other federal agencies for whom FPS has delegation oversight responsibility.

Information collected and stored in TAMS for FPS employees and contractors includes:

- Full Name (last name, first name and middle initial);
- Date of Birth;
- Social Security number (SSN);
- Age;
- Race;
- Height;
- Weight;
- Sex;
- State/Country of Birth;
- Home Address (including city, state, and zip);
- Mailing Address (including city, state, and zip);
- Emergency Contact (including last name, first name, middle initial);
- Relationship to student;
- Emergency Contact Phone Number;

- Emergency Contact Home Address (this information is optional and therefore does not have to be provided);
- Driver's License Number;
- Driver's License State;
- Military service; and
- Languages spoken.

Information collected and stored in TAMS for students who are employees of other federal agencies and whom FPS has delegation oversight responsibility includes:

- Full name (last name, first name, middle name);
- Organization name;
- City and State (of work location);
- Work telephone number;
- Work email address; and
- Type of training certification received.

TAMS will create several types of new information:

- Examination/Quiz/Observed Training Score
- Certification Award/Expiration
- Portfolio Management Linkage
- Inventory Linkage (This information is associated with inventory that is issued to a student. Examples of such inventory include body armor, weapons, holsters, and batons. This inventory would not be tracked in the official inventory system, Sunflower Asset Management System).
- Survey Results (Level I and Level III)[8]
- System and Employee Training Reports

[8] Level I surveys are those that are anonymous and focus on students' initial responses at the immediate conclusion of a class. Level II surveys are distributed to students and their supervisors to provide insight into how the class has impacted job performance. Level III surveys are used to evaluate the applicability of the class to job performance and are administered 6-12 months after the class conclusion. Not all Level III surveys will be anonymous as TPD needs to know who the student is, where are they located, and who their supervisor is to better evaluate the responses.

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

TAMS collects information from various sources but relies on two specific sources for priority data elements. The two primary sources are the NFC and directly from the individual TAMS user. Data that is collected in TAMS is used for the creation of personnel records and for the proper and effective tracking of training and certification requirements.

TAMS will receive biweekly data extracts from the NFC containing employee data such as SSN, first name, last name, middle initial, birth date, and Agency sub element codes from the NFC. These extracts will be imported automatically via data file transfers and uploads. No data will be returned to the NFC. The data will be used to provide pre-entered basic data and establish student profile accounts within TAMS for students who attend training. This data extract will only be performed for FPS employees/students, as it will reduce the data entry burden on academy/field personnel/system administrators.

Student profiles for FPS contractor employees will be established using existing contract vendor data reports. Such information is provided by contract program officers and designated contract training officers to the TAMS system administrator. The personal data belonging to contractor employees is derived from contractor on-boarding and training documentation. The data will be used to populate personnel records and to track current certification status of each contracted employee.

For students who are employees of other federal agencies and whom FPS has delegation oversight responsibility, the PII data elements are directly provided by the individual student. These data elements include full name, organization name, city/state or work location, work telephone number, and work email address. This information is provided to the system administrator in order to manually establish the student’s account and record in TAMS.

When an FPS employee or contractor accesses TAMS and he or she completes or exits a course, progress information, including the successful or unsuccessful course completion, is recorded automatically in TAMS.

As capabilities in TAMS expand in the future, FPS employees/contractors and external students will have the ability to log into TAMS to view their learning history, and will be able to make changes to their contact information to include: work address; telephone number; and emergency contact information. Any additional changes in which a student needs to update their records must be coordinated and requested through their training coordinator or program manager. This action is considered a human resources change request.

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

No commercially or publically sourced data will be utilized in TAMS. All TAMS data is derived from internal and vetted information sources such as the NFC Payroll Personnel System (PPS), local Human Resources (HR) data feeds, existing system data, and the individual user.

2.4 Discuss how accuracy of the data is ensured.

FPS relies on the accuracy of employee data that is received from the NFC. Individuals may verify their information/record within TAMS for accuracy if they are granted access to TAMS. Individuals may request corrections to their data by contacting their HR specialist for the correction of NFC PPS data, the TAMS system administrator for TAMS-related personnel record data, or contracted personnel may contact their contracting officer representative or the designated contractor TAMS administrator for the submission of corrections. The FPS TAMS system administrators conduct regular record audits to ensure the accuracy of student data in TAMS. FPS will have twelve primary TAMS administrators in addition to several that will be assigned to the eleven regional offices and FPS headquarters, all of which will be assigned to validate integrity checks. DHS ensures accuracy by retrieving information directly from the NFC PPS, which is the authoritative source system for DHS payroll processing.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that TAMS will collect more information than is typically needed to provide employee training and manage performance.

Mitigation: This risk is partially mitigated in that in some instances, TAMS does not require certain PII data elements that are collected, such as state/country of birth, race, sex, military service, and SSN in order to provide training or manage student performance. However many of these data elements are applicable for ensuring that the correct student receives the correct scores or certification to his or her student record. A student's SSN could serve as an identifier to ensure proper training certification recordation in TAMS. Some data elements such as languages spoken, military service, race, and/or sex are not required for administering training; however these data elements could be analyzed during TAMS reporting. FPS TPD thoroughly reviewed the necessary collection of data from students and implemented data minimization to only that which was necessary for the purpose of this program/system. Additionally, FPS will rely on technical safeguards within TAMS for the protection of the data collected, maintained, used, and disseminated. FPS will rely on existing DHS and NPPD policies and procedures for safeguarding PII. In addition, TAMS specific policies and procedures will be developed in coordination with the NPPD Office of Privacy to ensure compliance with those existing DHS and NPPD policies and procedures.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

Data imported from NFC will be used to provide pre-entered basic person record data and establish student profile accounts within TAMS for individuals attending training. This data extract will only be performed for FPS employees/students, as it will reduce the data entry burden on academy/field personnel/system administrators.

- The FPS Academy uses SSNs as unique identifiers for students attending training as required by the Office of Personnel Management. See Executive Order (EO) 9397: Numbering System for Federal Accounts Relating to Individual Persons provides the legal authority to use SSNs as unique identifiers.[9] The use of SSNs will allow FPS to ensure the accurate recording of an individual's training records so that there are no duplications within the system and to prevent accidental recording of data into another person's record. The training records will be used to verify and authenticate an individual's ability to work in law enforcement, and security for PSOs. It is critical, therefore, to ensure records are accurate as these records affect an individual's ability to perform assigned work.
- Home/mailing address is used for student correspondence. In the instances that it has been provided and in the event that it is needed, emergency point of contact home address can be used in the case of an emergency after other means of contact have not been successful.
- Race, height, weight, sex, and state/country of birth data is used for Equal Employment Opportunity Commission (EEOC) data requests. These data elements are not required to be provided.
- Driver's License Information is used to verify an individual's authorization to drive a Government Owned Vehicle.

Other data elements, such as military service and languages spoken, are used to populate the student's profile.

TAMS will need to collect name, organization name, city/state, work telephone number, work email, and type of certification received from students who are employees of other federal

[9] EO 13478 (November 20, 2008) amended EO 9397, making SSN use for such purposes discretionary.

agencies and for whom FPS has delegation oversight responsibility in order to ensure they have completed their required law enforcement trainings to perform their assigned duties.

TAMS-generated information (scores, test analysis, and class analytics) will be stored to the individual's record and to the TAMS class records; no new records will be generated from the derived data. If the collected data is derogatory, then it can be used to take administrative action against an individual for failure to meet established standards. These negative actions will be driven by current FPS training standards and policies. TAMS-generated data will be accessed by TAMS system administrators only and made available to the senior FPS leadership who will ultimately make the determination on how to act on the information based on applicable policies and procedures.

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.

TAMS will not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly. This not a normal function of FPS and will not be a function of the system.

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

TAMS is an FPS-specific system and will not be accessible to external components except on a case by case basis in very limited capacity. Such instances will include providing training completion reports, scores, examination results data, and survey data. All PII that is shared or transmitted will be obfuscated in accordance with prevailing privacy policies.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk for misuse of information by system users who have elevated system privileges.

Mitigation: All users have role-based access granted by system administrators. Systems administrators cannot modify their own system privileges. Role-based access controls grant elevated access by module. For example, Learning Management administrators who do not require access to performance management information do not have elevated access in the Performance Management module. This granular role and permission-based access helps prevent users with elevated privileges from accessing information beyond their need to know. TAMS has an audit log report that can be generated to track all system activities conducted by students and administrators.

Section 4.0 Notice

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

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

DHS provides notice on the collection of employee and contractor information as well as student information of those who are employees of other federal agencies. Notice is provided to all students by way of a TAMS-approved Privacy Act (e)(3) Statement, the SORNs listed in section 1.2 above, and through the publication of this PIA.

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

FPS employees/contractors and those whom FPS has delegation oversight responsibilities are aware, upon accepting a position with law enforcement responsibilities, of their assigned requirements and responsibilities that coincide with their employment. FPS Academy students are not required to provide their personal information for the purpose of using TAMS. Furnishing their PII data is voluntary. However, failure to furnish the requested information may result in ineligibility for participation in FPS training programs and/or errors in the processing of trainings they apply for or complete.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk employee and contractors are not aware that DHS is retrieving and using their PII from payroll, personnel security, and time and attendance systems.

Mitigation: This risk is partially mitigated through the publication of this PIA. In addition, DHS employees and contractors are provided with Privacy Act (e)(3) Statements when they complete the onboarding process with the Office of the Chief Human Capital Officer or their COR that provide notice that their personal information will be collected and maintained for a variety of purposes, including learning and performance management. FPS also provides notice to students via a DHS approved Privacy Act Statement. That notice explains to the user how their information is obtained and utilized within the system.

Section 5.0 Data Retention by the project

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

The training records in TAMS will follow the General Records Schedule 1, item 29 Training Records. 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 5 years old or 5 years after completion of a specific training program (NC1-64-77-10 item 30b1). Background and working files will be destroyed when 3 years old (NC1-64-77-10 item 30b2). Correspondence, memoranda, reports, and other records relating to the availability of training and employee participation in training programs sponsored by other Government agencies or non-Government institutions will be destroyed when 5 years old or when superseded or obsolete, whichever is sooner (NC1-64-77-10 item 30c).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than is required or needed.

Mitigation: This risk is mitigated through a retention feature within TAMS that is configured to automatically purge data in accordance with the NARA-approved retention schedule.

Section 6.0 Information Sharing

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

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

Internal student information belonging to FPS employees and contractors remains internal to DHS and is not shared outside of DHS as part of normal agency operations. External student information is not routinely shared outside of DHS; however there are limited instances in which an external agency may request training course completion status for their respective employees who have participated in FPS-sponsored trainings. In such instances, FPS personnel will manually transmit the specific student information to the approved external agency requestor.

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

TAMS will not routinely share data externally. However, upon request from external agencies, when their respective employees participate in FPS-sponsored training courses, a printed report can be provided to that agency indicating course completion data. This sharing is compatible with DHS/ALL-003 Department of Homeland Security General Training Records Routine Use L, which permits sharing with employers to the extent necessary to obtain information pertinent to the individual's fitness and qualifications for training.

6.3 Does the project place limitations on re-dissemination?

No. To the extent an external agency requests training course completion information for their respective employees, such information is released in accordance with an approved routine use and further limitations on re-dissemination are not necessary.

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

TAMS is an FPS-specific system and will not exchange or share information outside of the Department for those internal students who are FPS employees and contractors. If a request is made by an external agency for its respective employee’s training records, FPS will maintain an accounting of all such manual disclosures, which will be kept on file at the FPS Academy and Federal Law Enforcement Training Center (FLETC) Educational Aids Office.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Despite the limited nature of information sharing from TAMS, there is an inherent risk with sharing information externally.

Mitigation: This risk is partially mitigated by significantly limiting the sharing of information outside of FPS with respect to those students whom FPS has delegation authority. This sharing is done by way of a manual process once the external agency requestor has been verified to receive such information. In regards to internal FPS students’ records, although TAMS receives information (data extracts) from the NFC, TAMS does not return any data back to the NFC.

Section 7.0 Redress

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

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

Currently employees, contractors, and external students do not have direct access to their information contained within the system. As capabilities in TAMS expand in the future, FPS employees/contractors and external students will have the ability to log into TAMS to view their learning history, training records, and will be able to make changes to their contact information to include: work address; telephone number; and emergency contact information.

If an FPS employee or contractor has separated from the agency under normal circumstances, (i.e., found a new job, changed agency) he/she can request his/her training records through the FPS training/transcript retrieval request process.

If an employee has been terminated for any reason and is being represented by counsel on an EEO, Fair Labor Standards Act, or Merit Systems Promotion Board proceeding, a Freedom of Information Act (FOIA) request or discovery request will need to be requested through the FPS Legal Counsel or through the FPS FOIA request process.

External students/employees can request transcript and learning history reports through a request to the FPS TPD TAMS administrator.

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

Employees may request corrections to their data by contacting their HR specialist for the correction of NFC data and the TAMS system administrator for TAMS-related personnel record data. Contractor personnel may contact their contracting officer representative or the designated contractor TAMS administrator for the submission of corrections.

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

Individuals will be notified about change procedures through the agency internal communications protocol and through information links located in the system.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that inaccurate information will be maintained in the system.

Mitigation: This risk is mitigated by allowing individuals to request the correction of inaccurate information by contacting the user's HR specialist, contracting officer representative, or TAMS system administrator. A supervisor is required to verify and make appropriate changes if an individual feels his or her biographic or training information is inaccurate. They may also contact the TAMS helpdesk for assistance. As the system is further developed, individuals will be able to access the system and manually correct their information.

Section 8.0 Auditing and Accountability

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

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

FPS uses technical controls to ensure that information is used in accordance with the stated practices in this PIA. FPS uses role-based access controls to limit user's access to information. A student, specifically those who are employees or contractors to FPS, must have a valid and active DHS network account to access TAMS. TAMS also has full audit capability for all data changes in the system.

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

DHS provides mandatory privacy and security awareness training to all employees of the Department on an annual basis. This ensures that employees are aware of the necessary safeguarding practices when handling PII. Therefore the TAMS system administrator and FPS employees and contractors are trained on privacy practices. Additionally, TAMS administrators will be provided training and user guides to help them operate the system and safeguard the information therein. For all users (students) on-line user guides will be accessible within TAMS.

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 in the system is limited by user role. Regional training staff will only have access to their regional personnel and will have limited ability to alter information except to add training data to existing files. FPS TAMS administrators will have access to all system data and settings as well as all user information. All other users will be granted a read only access upon request and approval by the system owner.

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

The system is FPS-specific and will not share information with external agencies except through the manual download of reports for export upon request.

Responsible Officials

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

Approval Signature

Original signed copy of file with the DHS Privacy Office.

____

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