Privacy Impact Assessment
for the

eFLETC

DHS/FLETC/PIA-003

June 21, 2017

Contact Point

William H. Dooley
Chief, IT Business Management Division
Federal Law Enforcement Training Centers
(912) 261-4524

Reviewing Official

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

Abstract

The Federal Law Enforcement Training Centers (FLETC) is implementing eFLETC as a new virtual learning management environment supporting law enforcement training for federal, state, local, tribal, and international law enforcement officers. eFLETC will initially serve as a scheduling, instructional delivery, and records system for up to 14,000 students who may access eFLETC in the first year. The project automates and integrates processes to improve the efficiency of administrative support functions for online student training and registration, content delivery, and course analytics. FLETC is conducting this Privacy Impact Assessment (PIA) because, when fully implemented, eFLETC will collect, maintain, use, and disseminate personally identifiable information (PII) about all law enforcement officers who are registered users of the system.

Overview

The Federal Law Enforcement Training Centers (FLETC) serves a leadership role as the Federal Government's principal provider of world-class, interagency training of federal law enforcement personnel. FLETC prepares new and experienced law enforcement professionals to fulfill their responsibilities in a safe manner and at the highest level of proficiency. FLETC delivers interagency training with optimal efficiency through the government-wide sharing of facilities, equipment, and expertise that produces economies of scale available only from a consolidated law enforcement training organization. FLETC is in the process of architecting and developing an online training delivery capability that will provide law enforcement training and education in multiple delivery strategies and modalities.

FLETC currently provides law enforcement training to over 90 Partner Organizations. FLETC also trains state, local, tribal, campus, and international law enforcement officers and agents. The number of agencies attending training, the number of students trained, and the number of student-weeks delivered has steadily increased over the course of FLETC's history. FLETC's collaborative approach with its Partner Organizations uses research, training, and education in a shared mission of protecting our democratic institutions, ensuring public safety, and preserving law and order. More than 60,000 students are trained annually at FLETC training centers.

FLETC seeks to become a provider of virtual learning and services for the law enforcement community. FLETC is identifying and employing critical information technology (IT) and fiscal resources in focused and direct ways in an effort to forward the agency and Partner Organization's priorities and to ensure the success and optimization of eFLETC. eFLETC will contain FLETC student recordation data and personal information required for online training registration and transcription.

eFLETC consists of three discrete modules: Learning Management, Media Streaming Service, and Student Registration and Records. These modules are software hosted in a cloud that only contains eFLETC data at a vendor-managed datacenter. All vetted users will have access to the Learning Management and Media Streaming Service modules to complete their training requirements. Only eFLETC administrators will have access to the Student Registration and Records module.

eFLETC supports FLETC's increasing demand for law enforcement training by providing the ability to respond more quickly to the training needs of its customers with online training materials and courses readily available 24 hours a day, 7 days a week. eFLETC provides online registration capabilities for students and agency representatives. Records contained in eFLETC include schedules for eFLETC training programs and complete student training records. Current students are able to test online and retrieve their information electronically. Instructors and administrators can schedule classes and training resources, generate class rosters, assign instructors to classes, and assign students to various programs. eFLETC provides FLETC with a means to track the particular training that is provided, identify training trends and needs, schedule training classes and programs, schedule instructors, track training progress by students, assess the effectiveness of training, identify patterns, respond to requests for information related to the training of all eFLETC users, and facilitate the compilation of statistical information about training.

The Learning Management module manages the life-cycle of learning activities for all eFLETC students. It acts as the gateway for learners, trainers, supervisors, and administrators to access training. The Media Streaming module maintains and updates digital audio and video recordings, which can be associated with specific courses or provided as stand-alone informational pieces in the Learning Management module. The Student Registration and Records module maintains and updates user records, training histories, course catalogs, training resources, and training requirements. eFLETC also shares PII with FLETC's Student Administration and Scheduling System (SASS).[1]

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?

The authority to collect the information is derived from the Government Employees Training Act, 5 U.S.C. §§ 4101-4118 as implemented by Executive Order 11348 of April 20, 1969. Executive Order 11348 provides for training government personnel. Additionally, Executive Order 9397, as amended, permits federal agencies to use an individual's Social Security number (SSN) as a "permanent account number." The use of the SSN is appropriate because of the large number

[1] For more information about the FLETC Student Administration and Scheduling System (SASS), please *see* DHS/FLETC/PIA-002 Student Administration and Scheduling System (February 12, 2013), *available at* https://www.dhs.gov/privacy.

of present and former students who attend or have attended FLETC programs, who potentially may have identical names and dates of birth and whose identities can only be easily distinguished by SSN.

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

The student records contained in eFLETC are covered by the DHS Security General Training Records System of Records.[2] Information collected to allow access to eFLETC is covered by the General Information Technology Access Account Records System.[3]

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

No. The system is still in the development phase. It is anticipated that the system will be operational and have a signed Authority to Operate by September 30, 2017.

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

Yes. Student records contained within the system are retained for 40 years, in accordance with NARA-approved schedule N1-056-022, dated June 25, 2002.

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.

FLETC is in the process of completing an inventory of all information collections for eFLETC. FLETC will work with the Office of the Chief Information Officer (OCIO) Paperwork Reduction Act (PRA) Branch to complete this action.

Section 2.0 Characterization of the Information

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

The system will collect, generate, or retain the following types of information to create an individual's account:

[2] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

[3] *See* DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (November 27, 2012).

- Name;
- Social Security number;
- System-assigned unique identifier;
- Date of birth;
- Gender;
- Agency;
- Rank/title;
- Agency address;
- Agency fax number;
- Office phone (potentially home or personal cell phone if office phone has not been assigned);
- Office email (potentially personal email if office email has not been assigned);
- Student email (potentially personal email if agency email has not been assigned);
- Supervisor name;
- Supervisor email; and
- Legacy ID (this field will only be available to administrators).

Individuals will also be issued a username and single-use password to initially access eFLETC.[4]

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

Initially, the agency sponsoring the student enters basic student information into eFLETC. This action initiates a student record and serves as verification of the student's authorized user status. The information provided by the agency is obtained directly from the student. The system provides electronic notification of the registration to the students and provides directions for accessing the system to begin use.

Active students may take courses and tests and receive results through eFLETC. The system automatically scores tests upon completion and posts student grades to their records. All personal information within eFLETC is directly input by staff, students, or posted as an automated function of the system. eFLETC does not receive information or data from another system.

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.

[4] In the future, FLETC plans to allow students to access eFLETC with their DHS or agency-issued PIV cards.

2.4 Discuss how accuracy of the data is ensured.

Because information is obtained directly from students, who are provided the opportunity to complete and correct their data, it is assumed that information is correct. Sponsoring agencies will also have access to the information and will be afforded the capability of correcting inaccurate data. When students or their agencies cannot change data, the appropriate eFLETC staff may correct the record.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the student information maintained within eFLETC, specifically the collection and maintenance of SSNs, may increase exposure to identity theft or result in the mishandling of PII.

Mitigation: In addition to normal security measures such as role-based access, system auditing, and user training, FLETC has built specific safeguards into the system. eFLETC masks SSNs as soon as it captures the information. Only the student and limited FLETC personnel will have access to this information.

Privacy Risk: There is a risk that eFLETC will collect more information than is necessary to register an individual for training.

Mitigation: FLETC mitigates this risk by only collecting information necessary to support eFLETC's increasing demand for law enforcement training by streamlining current processes and providing the ability to respond more quickly to the training needs of its customers. FLETC uses information, such as SSN and sponsoring agency financial information, for academic recording (transcripts) only. FLETC reviews these collections every three years to ensure continued legal authority and necessity.

Privacy Risk: There is a risk that eFLETC will contain inaccurate information on training program/system applicants and students.

Mitigation: FLETC mitigates this risk by collecting, when possible, information directly from the student. Information within eFLETC is either collected directly from the student and submitted via the sponsoring agency, or is submitted directly by the student. FLETC assumes that the sponsoring agency maintains accurate information for its employees. Additionally, FLETC may contact the sponsoring agency points of contact to ensure information is correct.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

eFLETC requires name, date of birth, and SSN to accurately identify records relating to the student. For many students, their training results become part of the permanent records maintained by the student's sponsoring agency, Office of Personnel Management (OPM), Department of Labor, future employers, and educational institutions. Use of SSN allows for accurate matching with the student's permanent employment records. Students from some state and local agencies must submit an SSN to complete the billing and payment process when a sponsoring agency has an accounting system that requires an SSN for billing purposes. eFLETC also uses personal contact information to communicate with the student before, during, and after training.

Student performance data is recorded on a transcript and is used in virtually the same way as a college transcript. Student transcripts are routinely used to validate training and experience for job qualifications, college and university training credits, and establishing a student's knowledge base for a given situation in the law enforcement environment.

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

No. eFLETC does not use technology to locate a predictive pattern or anomaly. eFLETC queries only return reports to improve the training process. These reports include student rosters, individual student reports, and training results. De-personalized data from system queries may be used to evaluate the success of various training programs and determine patterns for successful completion based on student demographics such as age, gender, and experience. Aggregate data in the system is used only to evaluate and improve training programs and approaches.

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

Yes. Full implementation will enable eFLETC to share information with DHS, state, local, and other federal partners who enroll students at eFLETC. Electronically retrievable information will include student class assignments and participation. Hard copies of the entire student record may be made available to the sponsor upon written request for the purpose of performing background investigations and validating training.

Partner Organizations will access eFLETC and pre-register their students who require training, courses, and specific class dates for asynchronous and blended training opportunities. They will provide student names and SSNs as a part of the pre-registration process.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that FLETC will use the information it collects in eFLETC for non-training purposes, inconsistent with the original purpose for collection.

Mitigation: FLETC mitigates this risk through access controls, training, rules of behavior, and auditing. Only authorized users may access the information. Users must complete privacy and security training prior to receiving access to eFLETC. Individuals accessing or using the system for purposes other than what is required to administer training or exercise programs are restricted from accessing eFLETC.

Privacy Risk: There is a risk that users may gain unauthorized access to the system.

Mitigation: FLETC mitigates this risk through internal application-level, role-based access control for access to specific eFLETC functions. An eFLETC user only has access to information based on his or her role. Access to privileged functions for enforcing system/application access is restricted to authorized system administrators. Auditing is enabled across all components of the system in order to monitor and verify appropriate privilege usage on the system.

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.

The DHS/ALL-003 Department of Homeland Security General Training Records System of Records Notice (SORN)[5] and the publication of this PIA provide notice to the individual. Students also receive an electronic Privacy Notice during the online registration process describing why eFLETC is collecting this information.

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

The information eFLETC collects and maintains is required for all eFLETC students. For many government employees, eFLETC training may be a condition of employment as a law

[5] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

enforcement officer, and therefore mandatory. The Privacy Notice the user sees when providing the information will identify the routine uses of his or her information.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not know how FLETC uses his or her information, specifically the SSN.

Mitigation: FLETC mitigates this privacy risk by collecting registrant and applicant information directly from the individual as frequently as possible. FLETC also provides a Privacy Notice at the time of each collection. Additionally, FLETC provides notice through the DHS/ALL-003 Department of Homeland Security General Training Records SORN and this PIA.

Section 5.0 Data Retention by the project

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

Student information is retained for 40 years to remain retrievable throughout the active career of federal law enforcement agents. Student records and training schedules are retained to validate the type, duration, and extent of training provided to law enforcement officers. This provides a mechanism to validate training and experience for purposes of qualifying for jobs, obtaining training credit with colleges and universities, and establishing a student's knowledge base for a given situation in the law enforcement environment.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that FLETC may maintain the information collected, specifically SSN, for a longer period than necessary.

Mitigation: Although there is always risk inherent in retaining PII for any length of time, the retention periods identified in the NARA schedule are consistent with the concept of retaining data only for as long as necessary to support the agency's mission. This risk is mitigated by purging or transferring records as required by the NARA-approved record schedule by the sponsoring FLETC training and/or exercise program.

FLETC retains SSN for the NARA-approved retention period (40 years) for several reasons. Regardless of whether the student is affiliated with DHS or a Partner Organization, SSN is the only unique identifier that can be used to retrieve the individual's record. FLETC needs to retain SSN to match records of students who come back for multiple programs over the lifetime of their career or move in and out of law enforcement officer positions. Also, if during a law enforcement activity (*e.g.*, an officer-involved shooting), an officer's training could be called into question by an agency or during a legal proceeding. The relevant training could include records from years prior to the incident. In addition, FLETC often receives requests from former students who would like to obtain copies of their training records for use when applying for other law enforcement positions, seeking college credit for training received at FLETC, and documenting service.

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.

The sharing of PII outside the Department is part of normal operations and is compatible with the original collection of information and the routine uses in the published DHS/ALL-003 Department of Homeland Security General Training Records SORN.[6] Agencies that sponsor students in eFLETC can access the system based on their system access permissions, in order to provide and receive information about their students. Students can also access their profiles in order to access their own information. The primary uses of sharing include validating training, evaluating the need for further training, and establishing the training level of students for position qualification or educational background.

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

While all listed routine uses may be applied to these records, FLETC generally shares training information connected to the hiring or retention of an employee with OPM, educational institutions, or training facilities to verify employee attendance and performance.[7] The sharing supports the training, educational, and professional development purposes for which the system was developed.

[6] *See* DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).

[7] The routine uses in the DHS/ALL-003 Department of Homeland Security General Training Records SORN that describe this sharing include: (H) To a Federal, State, tribal, local or foreign government agency or professional licensing authority in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance or status of a license, grant, or other benefit by the requesting entity, to the extent that the information is relevant and necessary to the requesting entity's decision on the matter; (I) To educational institutions or training facilities for purposes of enrollment and verification of employee attendance and performance; and (J) To the Equal Employment Opportunity Commission, Merit Systems Protection Board, Office of the Special Counsel, Federal Labor Relations Authority, or Office of Personnel Management or to arbitrators and other parties responsible for processing any personnel actions or conducting administrative hearings or appeals, or if needed in the performance of authorized duties.

6.3 Does the project place limitations on re-dissemination?

Yes. Information may not be disclosed outside of the sharing outlined in the DHS/ALL-003 Department of Homeland Security General Training Records SORN without the written permission of the individual or the FLETC Disclosure Office.

For all other external sharing of information, FLETC will either include a letter to the organization or execute an information sharing and access agreement such as a Memorandum of Understanding (MOU) with the external agency. This sharing could be with another federal agency, and FLETC would indicate that FLETC's Privacy Act records being provided or transferred are for use pursuant to applicable routine uses and that further disclosure of the records is not permissible.

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

FLETC maintains paper and electronic copies of all requests for records and the agency’s response to the request. Additionally, requests for information within the system are made to the FLETC Disclosure Office or FLETC Educational Aides Office that maintain the accounting of what records were disclosed and to whom under the Privacy Act and Freedom of Information Act.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that FLETC and Partner Organizations will further disclose information contained within eFLETC.

Mitigation: FLETC mitigates this risk because eFLETC is not connected to any external systems to facilitate regular or bulk sharing. All information is shared on a case-by-case basis as authorized by law and FLETC provides notice that the information may not be re-disseminated. FLETC provides the academic records directly to the student upon his or her written request. The student may then share the information at his or her own discretion.

Section 7.0 Redress

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

In addition to the direct access provided to users with an active account, individuals may submit a written request in accordance with the Privacy Act and Freedom of Information Act to the FLETC Disclosure Officer. These requests should be directed to:

Federal Law Enforcement Training Center
FOIA/Privacy Request
1131 Chapel Crossing Road, Building 681
Glynco, Georgia 31524

Inquiries may also be initiated through the FLETC website, www.fletc.gov.

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

The FLETC website provides direction to individuals for correcting the information contained in FLETC records.[8] Written requests should be directed to:

Federal Law Enforcement Training Center
FOIA/Privacy Request
1131 Chapel Crossing Road, Building 681
Glynco, Georgia 31524

Inquiries may also be initiated through the FLETC website, but only procedural information is exchanged in this manner. No action will be taken to correct a record without a signed, written request, proof of identity, and proof that the information in question is inaccurate.

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

FLETC provides general notice to the individual about correcting his or her information on the FLETC website. The instructions direct the individual to contact the FLETC Disclosure Office with his or her written request and supporting documentation.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that the individual may be unable to correct his or her information once he or she provides it to FLETC.

Mitigation: FLETC mitigates this risk by allowing an individual to correct his or her information: 1) through a telephone call to the appropriate Support Services Center (or Help Desk); 2) by accessing his or her record electronically, such as via a web-based interface using a user ID and password; and 3) by allowing access and correction through the procedures outlined in the DHS Privacy Act Regulations, 44 CFR Part 6 and 6 CFR Part 5.

[8] For more information, please *see* https://www.fletc.gov/guide-foia-privacy-act.

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?

FLETC uses technical controls to ensure that information is used in accordance with the stated practices in this PIA. eFLETC uses role-based access controls to limit user's access to information. An individual must have a valid and active eFLETC account to access the system. eFLETC 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.

All eFLETC users (i.e., instructors, system administrators, training support staff) must have both annual privacy and IT security training prior to receiving access to the system. Those with security responsibilities receive training dealing with elevated privileges. Those, such as System Owners and Information System Security Officers, receive role-based training related to their security functions.

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

eFLETC controls data access through domains and workflows (a role is a collection of workflows). A domain defines the data a user can access; a workflow establishes what the user can do with that record in the database. Domain access and user roles are configured in the system according to the business requirements set forth by the Program Manager. These business decisions are documented in the eFLETC design documentation. Access to eFLETC falls in four general categories: (1) students; (2) administrative users; (3) Partner Organization users; and (4) system administrators including database administrators, network engineers, etc.

Once they have been registered for training in eFLETC, the system generates an e-mail to the student that includes the student's login information. The eFLETC administrator grants access to administrative users at the request of the user's supervisor or contracting officer's representative. The request must specify the level of access required and verify the user's need-to-know. If approved, an account is created and a role is assigned to the user. eFLETC grants access to Partner Organization users as determined in the MOU laying out use of the system..

System administrators are responsible for the actual software and hardware on which eFLETC operates. Personnel having system level access to the eFLETC must first submit to a background investigation and go through the government security clearance process. These procedures are documented in the System Security Plan.

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?

FLETC establishes data sharing agreements with external entities using Interconnection Security Agreements (ISA), MOUs, and Interagency Sharing Agreements. DHS Sensitive Systems Policy Directive 4300A establishes this requirement for DHS systems. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems permit only acceptable transactions. The ISA includes descriptive, technical, procedural, and planning information. The ISA also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The DAA for each organization is responsible for reviewing and signing the ISA.

Responsible Officials

William H. Dooley
Chief, IT Business Management Division
Federal Law Enforcement Training Center
Department of Homeland Security

Approval Signature

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

____

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