Privacy Impact Assessment
for the

Enterprise Security System (ESS)

January 25, 2010

Contact Point
Marty Zimmerman-Pate
Privacy Officer
DHS/FLETC
(912) 267-3103

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Federal Law Enforcement Training Center (FLETC) is launching the Enterprise Security System (ESS). ESS will standardize the process for students, contractors, visitors, and personnel to obtain access to FLETC facilities. This PIA is being conducted because personally identifiable information (PII) will be collected and maintained on students, visitors, and personnel.

Overview

FLETC provides basic and advanced law enforcement training to more than 82 federal, state, local, and international law enforcement organizations (generally referred to as Partner Organizations). More than 60,000 students are trained annually at FLETC sites, requiring secured access to both FLETC sites and registration information. To properly control access to FLETC facilities and information, individuals must wear identification issued by the Security and Emergency Management (SEM) Division at all times. The information in ESS will be used to issue photo identification badges and credentials, parking permits, and visitor badges.

FLETC uses multiple forms to collect the PII contained within ESS. The PII pertains to students, contractors, visitors, and personnel of FLETC. Students who train at FLETC may return many times throughout their law enforcement careers. Visitors may be friends or family members of students or personnel who attend student events or visitors seeking information from or consultation with FLETC personnel. Information will only be collected from students, contractors, visitors, and personnel of FLETC.

The following steps describe a typical student applicant transaction in ESS:

1. Student is scheduled for training at FLETC.
2. Student completes required application and registration form.
3. Form is sent to SEM Division for badge issuance, data validation, and background check.
4. Completed form is sent to SEM Division for personnel security processing.
5. If a student has previously attended FLETC, their file is pulled from ESS and the data is updated as needed. If not, information is entered into ESS in full by SEM Division personnel.

The functions performed by ESS were previously performed manually, or by various stand-alone systems with no interconnectivity. These functions include a general background check, driver license validation, and similar verifications to establish the identity and suitability of students, personnel, and visitors. Each FLETC site used a different system or program to generate identification cards, which must be worn when on-site. With the launch of ESS, these functions will be performed under the auspices of one system.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as the reasons for its collection as part of the program, system, rule, or technology being developed.

1.1. What information is collected, used, disseminated, or maintained in the system?

The following information will be collected from students, contractors, visitors, and personnel seeking to gain access to FLETC facilities. Individuals visiting FLETC students, contractors, and personnel will be sponsored and checked in on a daily basis. They will not be processed through ESS.

Students	**Contractors and Visitors**	**Personnel**
Name	Name	Name
Social Security Number	Social Security Number	Social Security Number
Date of Birth	Date of Birth	Date of Birth
Home address	Home address	Home address
Agency	Employer	Office
Position	Position	Position
Emergency Contact Information	Emergency Contact Information	Emergency Contact Information
Drivers License Number	Drivers License Number	Drivers License Number
Housing Assignment	Citizenship	Photograph
Photograph	Photograph	

The system creates and assigns a unique number for each card issued. In addition to the information above which is obtained directly from the individual, the system will contain positive or negative outcomes from background checks, and any annotations concerning access restrictions.

1.2. What are the sources of the information?

The PII will be collected directly from individuals seeking access to FLETC. Each form contains a Privacy Act Statement and is outlined in Appendix A. The information will be manually entered into the system by the SEM Division personnel. Completed forms will be used to perform background investigations and only the background check results will be recorded in ESS. Original documents required to process applications for employment and access to FLETC are maintained by the Personnel Security Branch of the SEM Division in accordance with DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081).

1.3. Why is the information being collected, used, disseminated, or maintained?

The information will be collected from individuals to: identify those seeking access to FLETC facilities; complete background checks; and provide emergency contact information. Citizenship is collected from contractors and foreign national visitors to meet DHS foreign visitor vetting requirements.

1.4. How is the information collected?

Individuals seeking access to FLETC facilities will complete the appropriate FLETC forms, some of which may be submitted electronically. Individuals may also send or bring hard copies of the completed forms to FLETC. Information identified in Section 1.1, along

with results of the background check, will be entered into ESS by SEM Division personnel once verification has been completed.

1.5. How will information be checked for accuracy?

Information provided by the individual will be assumed to be accurate. If, in the process of performing necessary verifications, there appear to be inaccuracies, the individual will be contacted by SEM Division personnel and provided an opportunity to clarify or correct the information.

1.6. What specific legal authorities/arrangements/agreements define the collection of information?

FLETC's legal authority to operate and administer training programs can be found in 6 U.S.C. §§ 464-464e, and Memorandum of Understanding for the Sponsorship and Operation of the Consolidated Federal Law Enforcement Training Center, dated September 30, 1970, as amended. Executive Order 11348 provides for training government personnel.

Executive Order 9397, as amended, allows federal agencies to use an individual's Social Security Number as their "permanent account number." At FLETC, the SSN will be used only as necessary in connection with processing student records and financial transactions. The use of the SSN is made necessary because of the large number of present and former students who attend or have attended FLETC Programs, and who potentially may have identical names and dates of birth and whose identities can only be distinguished by SSN.

Authority to maintain records associated with DHS facility and perimeter access control, including visitor management can be found in 5 U.S.C. § 301; the Federal Records Act, 6 U.S.C., the Homeland Security Act; 44 U.S.C. § 3101; and Executive Order 9397, as amended; Executive Order 12968, Federal Property Regulations, issued July 2002.

1.7. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a risk that some PII collected in ESS will be inaccurate. The risk associated with ESS's retention of inaccurate PII is mitigated by the fact that information is collected directly from the individual.

There is also a risk that more information will be collected than is necessary for the program. To reduce the risk, only information needed for the required background checks and issuance of badges and credentials will be collected.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information in ESS will be used to:

- Conduct background checks to ensure safety and security of FLETC sites and personnel;
- Create an identification badge to be worn at all times while on a FLETC site;
- Contact family and employer in case of emergency;
- Establish eligibility for driver-related training and driving privileges while at the FLETC; and
- Perform investigative or law enforcement activities as required, such as vehicle accidents, injury accidents, alleged misconduct, etc.

2.2 What types of tools are used to analyze the data and what type of data may be produced?

The system will not analyze data.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system will not use or collect commercial or publicly available data; only data provided by individuals and the final result of the background investigation. The scope of a background investigation determines whether commercial and publicly available data will be collected, however, commercial and publicly available data is not captured or used by ESS. For more information on background investigations, please consult DHS/ALL – 023 Personnel Security Management System of Records (January 16, 2009, 74 FR 3084).

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There is a risk that users who do not have a need to know will access ESS information. To mitigate this risk, the SEM Division has mandated that only privileged users of ESS will have access to information. Information is maintained within the system only. Hard copy forms are destroyed upon final adjudication of the access request.

For current records, file permissions protect retention information from unauthorized access, modification, and deletion.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Information maintained within the system will be destroyed no later than five years after the expiration of the relationship with the individual requesting access or upon notification of death. Identification credentials including cards, badges, parking permits,

photographs, agency permits, and visitor passes will be destroyed three months after return to the issuing office.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

These records will be maintained in accordance with General Records Schedule (GRS) 18, Item 22a and GRS 11, Item 4a.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Many visitors to FLETC return periodically. Personal information may change frequently, and information contained in the system may become inaccurate. To mitigate this risk, the records of individuals that return to FLETC will be updated and then maintained only as required. The opportunity to change and verify PII each time access is renewed minimizes the risk that inaccurate information will be maintained.

Furthermore, the retention schedule established above mitigates the risk that information of any kind will be retained indefinitely.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared, what information is shared and for what purpose?

Any information contained within the system may be shared within DHS for personnel security purposes or with those individuals demonstrating a need to know.

4.2 How is the information transmitted or disclosed?

Information sharing requests are received in writing or in person. Information may be disclosed in hard copy, electronic copy, or verbally upon receipt of a valid request from an authorized agent of the requesting agency. Information will be made available in the format requested.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

There is a risk that information will be inappropriately disclosed. To mitigate this risk, SEM Division personnel will limit access to information within ESS to individuals who have demonstrated a need to know. Furthermore, the destruction and/or deletion of information mandated in the retention schedule also reduces the risk that PII will be inappropriately disclosed.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared, and for what purpose?

Information contained in ESS will be shared externally to accomplish the required suitability determinations, in connection with an investigation, or legal or administrative proceedings that require the information. This is a manual process and there is no interconnectivity or data matching. Only SEM Division personnel share information with external organizations.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of PII outside the Department is compatible with the original collection of information. The primary uses include validation of suitability and background investigations to determine level of access. External sharing is consistent with the routine uses published in DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081).

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information shared in accordance with routine uses published in DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081) will be transmitted verbally or in hard copy. Direct communication between FLETC personnel and the appropriate agency will occur to provide the necessary information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The risk is that information transmitted would be misunderstood or not provided within context. This risk will be mitigated when SEM Division personnel provide the information and can give context to those performing enforcement activities. There is further risk that the information will be compromised. The risk will be mitigated by restricting information in the system to those performing enforcement.

SECTION 6.0 NOTICE

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes, notice is provided through this Privacy Impact Assessment, the DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081), as well as through Privacy Act Statements at the point of collection.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. However, individuals who decline to provide the required information will not be granted access to FLETC facilities.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

Records are shared consistent with published routine uses in DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081). For uses not covered under this SORN, the subject of the records must authorize the release in advance of sharing.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There is a risk that lack of notice will be provided to individuals. This risk is mitigated when individuals are provided a Privacy Act Statement on the form used to collect their information. Because this information is used solely to provide individual identification in order to access FLETC facilities, there will be no instances in which the individual is unaware of the collection of this information and its intended use.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Individual requests for records may be submitted in writing to the Disclosure Office. Requesters are provided instructions for submitting requests on the FLETC.gov website. Requests should be addressed to the Privacy and Disclosure Officer, Federal Law

Enforcement Training Center, 1131 Chapel Crossing Road, Building 681, Glynco, Georgia 31524. Access procedures are also outlined in DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081).

7.2 What are the procedures for correcting inaccurate or erroneous information?

See 7.1.

7.3 How are individuals notified of the procedures for correcting their information?

Correction notification procedures are outlined in DHS/ALL -024 Facility and Perimeter Access Control and Visitor Management System of Records (January 16, 2009, 74 FR 3081).

7.4 If no formal redress is provided, are alternatives available to the individual?

Redress is provided. See 7.1.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There is risk that individuals will not be permitted access FLETC due to inaccurate information provided. This risk is mitigated when information is provided directly from individuals to FLETC for the sole purpose of gaining access to training sites. If for any reason the individual is denied access and requests a copy of the record used to make this determination, they will be directed to the Privacy and Disclosure Officer, Federal Law Enforcement Training Center, 1131 Chapel Crossing Road, Glynco, Georgia 31524. If the issue is not resolved to the individual's satisfaction through this process, an appeal may be submitted to the Director, Federal Law Enforcement Training Center.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Access to this system will be determined by the individual's duty and role. Only SEM Division personnel will have access and will be required to complete both Privacy and IT Security Training prior to access being granted. There are also Rules of Behavior that must be completed and signed before access is granted. The procedures for granting access are outlined in FLETC Directive and Manual 4900, Information Technology System Rules of Behavior and Use Agreements.

8.2 Will Department contractors have access to the system?

Department contractors who require the information to perform their duties will have access to the system. Training requirements are the same as for FLETC personnel. Before contractors may be granted access, non-disclosure agreements must be in place either through appropriate contract language and obtaining a signed non-disclosure agreement.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All users must complete both privacy and IT Security training prior to being granted access to the system and annually thereafter.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The C&A was submitted to DHS and granted Authority to Operate on May 19, 2009.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Access roles are determined by managers and will be reviewed periodically to ensure that users have the appropriate access. Access will be audited and the audit logs reviewed on a regular basis.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There is a risk that data will be lost or inappropriately disclosed. This risk is mitigated by existing procedures that outline appropriate controls to obtain access to the system, the auditing capabilities of the system, and the restrictions placed on downloading, transferring, and printing information.

Audit logs that document system and user activity will be reviewed periodically and any inappropriate or questionable activity will be investigated and appropriate action taken.

ESS uses the following controls:

- Access will be limited to trained SEM Division personnel;
- Users must take Privacy and IT Security Training prior to being granted access to the system;
- Systems will be maintained in secured areas with limited access; and
- Passwords will meet system-defined criteria.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The ESS system is a commercial off-the-shelf system.

9.2 What stage of development is the system in and what project development lifecycle was used?

The ESS is currently in the operational stage of its System Development Life Cycle.

9.3 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data is encrypted using Triple Data Encryption Standard (DES). Triple DES provides a relatively simple method of increasing the key size of DES to protect against brute force attacks, without requiring a completely new block cipher algorithm. Data at rest is the methodology used to store data on the server. Privacy at the workstation is addressed through policy.

9.4 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No. Multiple federal agencies including the Internal Revenue Service and the U.S. Air Force use this system.

Approval Signature

APPROVAL SIGNATURE

Original signed and on file with the DHS Privacy Office
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A

Examples of Privacy Act Statements

PRIVACY ACT STATEMENT (employee badge application form)

This information is provided in accordance with the Privacy Act of 1974 (5 USC § 552a). Authority for this information is 5 USC § 301, 5 USC § 4101 et seq. Executive Order 11348 and Department of Homeland Security Delegation Number 7050. Disclosure of this information is voluntary. Failure to provide requested information may result in denial of access to the FLETC.

PRIVACY ACT STATEMENT (student registration form)

Authority

The authority to collect the information is derived from the Government Employees Training Act, 5 USC §§ 4101-4118 as implemented by Executive Order 11348 of April 20, 1969, Reorganizing Plan No. 26 of 1950, the Department of the Treasury Order No. 140-01(Federal Law Enforcement Training Center), and Memorandum of Understanding for the Sponsorship and Operation of the Consolidated Federal Law Enforcement Training Center.

Purpose and Uses

The information you supply will be used to assist the government in retrieving information documenting your training. If you furnish none of the information requested, your attendance in training will be immediately terminated. These records and information in the records may be used to: (1) disclose pertinent information to appropriate federal, state, local or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation; (2) disclose information to a federal, state, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit; (3) disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence. Other routine uses can be found in DHS/All-003 - Department of Homeland Security General Training Records (November 25, 2008, 73 FR 71656).

Effects of Nondisclosure

If you furnish only part of the information required, an attempt will be made to maintain and process your records. If the information withheld is found to be essential to effectively maintaining and processing your records, you will be so informed, and your training will terminate unless you supply the missing information.

Disclosure of your Social Security Number (SSN)

Disclosure by you of your SSN is not mandatory. Solicitation of the SSN is permitted under the provisions of Executive Order 9397, as amended. The SSN will be used only as necessary in connection with retrieving your records. The use of the SSN is made necessary because of the large number of present and former students who attend or have attended FLETC Programs, and who potentially may have identical names and dates of birth and whose identities can only be distinguished by the SSN.