



Privacy Impact Assessment  
for the

# Student Administration and Scheduling System

DHS/FLETC/PIA-002

**February 12, 2013**

**Contact Point**

**William H. Dooley**

**Chief, Office of IT Budget, Policy, & Plans  
Federal Law Enforcement Training Center  
(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 Center (FLETC) is implementing the Student Administration and Scheduling System (SASS). SASS serves as a scheduling and records system for more than 60,000 students who attend FLETC each year. The project automates and integrates myriad manual processes to improve the efficiency of administrative support functions for student training and registration. This Privacy Impact Assessment (PIA) is required as the system contains personally identifiable information (PII).

## Overview

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. Training consists of all phases of law enforcement instruction, from firearms and high-speed vehicle operations, to legal case instructions and defendant interview techniques. FLETC delivers interagency training with optimal efficiency through the government-wide sharing of facilities, equipment, and expertise which produces economies of scale available only from a consolidated law enforcement training organization. The consolidated training approach allows FLETC to respond quickly to emerging training needs, readily adapt to new requirements, and focus exclusively on training.

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 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.

SASS supports FLETC'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.<sup>1</sup> SASS provides online registration capabilities for students and agency representatives. SASS contains personally identifiable information about students and FLETC staff members. Records contained in SASS include: schedules for FLETC 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. SASS 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 items issued to students, assess the effectiveness of training, identify patterns, respond to requests for information related to the training of DHS personnel and other individuals, and facilitate the compilation of statistical information about training.

---

<sup>1</sup> Consistent with the Federal Law Enforcement Training Center Strategic Plan FY 2008-2013, December 18, 2007, Objective 1.6.1 "Implement the Student Administration and Scheduling System (SASS)" to enhance training management processes, available at <http://www.fleetc.gov/about-fleetc/strategicplan.pdf/view>.



The new functions performed by SASS replace existing manual processes and stand-alone systems with no interconnectivity. SASS implementation integrates these functions into a single system that interfaces with FLETC's financial and physical access security systems. SASS reduces the need for redundant information and provides a more secure and efficient means of administering training programs. In addition, SASS allows students to access and update their own information via the internet. SASS also allows authorized agency points of contact to enroll students for classes, retrieve student training information, and review student training history.

The process begins when a sponsoring agency submits a request for training slots to FLETC. FLETC then approves the training slots based on its availability. Sponsoring agencies generally identify a point of contact (POC) who will obtain access to SASS, with FLETC approval. Generally the POC enters information into SASS about the trainee; however, when an agency does not have an account, FLETC Training Resource Coordination Division staff will enter the trainees' information that the sponsoring agency provides. For new students, the sponsoring agency POC or a FLETC staff member builds a profile for the student containing basic information such as name, address, email address, organizational affiliation, and class. Students receive an email indicating they have been registered for class and instructing them to provide additional registration information via the internet. At this time, students are provided a login and password. The password must be changed at log-in. Once logged on, the student has the ability to update and correct his or her registration record. This record includes name, date of birth, Social Security Number (SSN), home address, emergency point of contact, driver's license number, personal email address, and telephone numbers. The personally identifiable information (PII) contained within SASS pertains only to students and staff of the Federal Law Enforcement Training Center.

FLETC identified and mitigated several privacy risks associated with SASS. Generally, the privacy risks associated with SASS are: 1) the collection of student information, including the SSN, may increase exposure to identity theft or may result in the mishandling of PII; 2) the collection of student information may include more information than necessary to accomplish FLETC's training goals; 3) SASS may contain inaccurate information about student; and, 4) students may not be aware of FLETC's collection and uses of their information.

FLETC mitigates these risks through security measures such as role-based access controls, system auditing, user training, and building specific safeguards into the system. Role-based access within SASS ensures that only individuals who require access to information in order to perform their duties will be able to review and edit student information. The data within the system resides on a secure server within the FLETC network. In order to ensure that information is secure, the system provides routine electronic audit results that are reviewed by the Information System Security Officer. SASS also masks SSNs and limits access to the student and limited FLETC personnel. FLETC limits the collection of information in SASS to only information that is necessary to carry out its training mission. SASS collects, when possible, information directly from the student, and allows students the opportunity to correct information by providing students with access to the system. Additionally, FLETC provides individuals with notice, with each information collection to ensure that individuals are aware of the purpose for the collection and the uses of the information.



## **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, 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.

Executive Order 11348 provides for training government personnel. Executive Order 9397, as amended, allows federal agencies to use an individual's SSN as a "permanent account number." 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 accurately distinguished by the SSN.

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

The student records contained in SASS are covered by DHS/All-003 - Department of Homeland Security General Training Records, November 25, 2008, 73 FR 71656.

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

Yes. The current system security plan was validated by the DHS Office of the Chief Information Security Officer on December 2, 2011.

### **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 covered by NARA approved schedule N1-056-022, approved on 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.**

Personal information contained in the system is gathered from law enforcement agencies registering their employees as prospective FLETC students, or from the students themselves, seeking training to perform their law enforcement mission and is not covered by the Paperwork Reduction Act.



## Section 2.0 Characterization of the Information

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

The table below identifies personal information gathered or stored in SASS. SASS will only contain information for FLETC students and staff members.

| Students                         | Staff                  |
|----------------------------------|------------------------|
| Name                             | Name                   |
| SSN                              | Division/Branch        |
| Gender                           | Qualifications         |
| Date of birth                    | Instructional Schedule |
| Full home address                | Cell phone             |
| Agency                           |                        |
| Position                         |                        |
| Emergency contact information    |                        |
| Personal email address           |                        |
| Telephone number(s)              |                        |
| Driver's license number          |                        |
| Driver's license expiration date |                        |
| Housing assignment               |                        |
| Exam results                     |                        |
| Student transcript               |                        |

SASS will provide automated testing and scoring functionality. Students will be able to take exams online and the system will automatically score and record the results of the test.

### 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 SASS. This action initiates a student record and serves as verification of the student's authorized attendance. 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 complete the registration process.

Student account access expires upon completion of the training; once a student leaves the facility FLETC discontinues account access within 24 hours. FLETC will renew access for a returning student allowing him or her to update personal information prior to reporting for follow-on classes.

Active students may take tests and receive results through SASS. The system automatically scores tests upon completion and posts student grades to their records. All personal information within SASS is directly input by staff, students or posted as an automated function of the system. It 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. All data is provided directly or indirectly by the student or is information pertaining to the student that is generated during the course of training.

## **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 in SASS, the appropriate FLETC staff may correct the record.

## **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

**Privacy Risk:** There is a privacy risk that the student information maintained within SASS 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. SASS 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 privacy risk that SASS 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 FLETC'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), and to reimburse or arrange invitational travel for training participants only. FLETC reviews these collections every three years to ensure continued legal authority and necessity.

**Privacy Risk:** There is a privacy risk that SASS 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 SASS 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.**

SASS requires name, date of birth, and SSNs to accurately identify records relating to the student. FLETC training is an employment requirement for many students and their training results become part of the permanent records maintained by the student's sponsoring agency, Office of Personnel Management, Department of Labor, future employers, and educational institutions. Use of the 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. FLETC 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, SASS does not use technology to locate a predictive pattern or anomaly. Queries only return reports FLETC will use during the training process. These reports include student rosters, lodging assignments, individual student reports, and physical 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?**

Full implementation will enable SASS to "share" information with DHS partners who sponsor students at FLETC. Electronically retrievable information will include student class assignments and attendance. 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 SASS and input their training needs, i.e., number of students that require training, courses, and specific class dates. They will also access SASS for scheduled classes to provide student names and SSNs as a part of the pre-registration process.

FLETC maintains a current list of Partner Organizations on its website, [www.fletc.gov](http://www.fletc.gov). Current DHS Partner Organizations include:

- Federal Air Marshal Service



- Federal Emergency Management Agency, Office of Security
- Federal Protective Service
- Office of Inspector General
- Transportation Security Administration
- U.S. Citizenship and Immigration Services
- U.S. Coast Guard
- U.S. Customs and Border Protection (including the U.S. Border Patrol)
- U.S. Immigration and Customs Enforcement
- U.S. Secret Service

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a privacy risk that FLETC will use the information it collects in SASS 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 SASS. Individuals accessing or using the system for purposes other than what is required to administer training or exercise programs are restricted from accessing SASS.

**Privacy Risk:** There is a privacy 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 SASS functions. A SASS 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 System of Records Notice for DHS/All-003 - Department of Homeland Security General Training Records November 25, 2008, 73 FR 71656 and the publication of this PIA provide notice to the individual. Students also receive an electronic Privacy Act Statement describing why FLETC is collecting this information during the online registration process.



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

The information SASS collects and maintains is required for all FLETC students. For many government employees, FLETC training is a condition of employment as a law enforcement officer, and therefore is mandatory. The Privacy Act 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 privacy 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 Act notice at the time of each collection. Additionally, FLETC provides notice through the DHS/ALL-003 Department of Homeland Security General Training Records System of Records Notice 73 FR 71656, November 25, 2008 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 so as 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 privacy risk that FLETC may maintain the information collected 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 privacy 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.



## 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 SORN. Agencies that sponsor students to attend FLETC can access SASS based on their system access permissions, in order to provide and receive information about their students. Students can also access SASS in order to access their own information. The primary uses include validating training, evaluating the need for further training, and establishing the training level of prior 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 the Office of Personnel Management, educational institutions, or training facilities to verify employee attendance and performance.<sup>2</sup>

### **6.3 Does the project place limitations on re-dissemination?**

Information may not be disclosed outside of the sharing outlined in SORN DHS/All-003-Department of Homeland Security General Training Records, November 25, 2008, 73 FR 71656 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 with the external agency such as with another federal agency indicating that FLETC's Privacy Act records provided or are being transferred for use pursuant to applicable routine uses and that further disclosure of the records is not permissible.

---

<sup>2</sup> DHS/All-003 - Department of Homeland Security General Training Records, November 25, 2008, 73 FR 71656 Routine Uses: (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.



## **6.4 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 who 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 privacy risk that FLETC and Partner Organizations will further disclose information contained within SASS.

**Mitigation:** FLETC mitigates this risk because SASS is not connected to other 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 the 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](http://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.<sup>3</sup> Written requests should be directed to the 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.

---

<sup>3</sup> For detailed information on how to initiate a FOIA or Privacy Act request, please see <http://www.fletc.gov/reference/public-information/freedom-of-information-act-foia/>.



### **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 privacy risk that the individual may be unable to correct his/her information once he or she provides it to FLETC.

**Mitigation:** FLETC mitigates this risk by allowing an individual to correct his/her information: 1) through a telephone call to the appropriate Support Services Center (or Help Desk); 2) by accessing his/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.

## **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?**

In order to minimize or mitigate the risk of unnecessary or inappropriate use of information, SASS uses the following controls:

- Access must be requested through supervisor;
- Users must take privacy training prior to being granted access;
- User names are assigned by the system;
- Passwords must meet system-defined criteria;
- Access is role-based and determined by user profile;
- Printing/downloading is limited;
- SSNs are entered upon initial registration, then masked within the system;
- Access to SSNs is tightly controlled;
- Student users are only able to access their own information;
- Only users with an official need to know, designated by the SASS program manager, will be able to access sensitive information once a student is registered; and
- Web based access and data exchange of information to and from SASS is encrypted.

After initial entry, student users cannot query their information by social security number or even see their SSN when other information is displayed. Access to SSN information in SASS is limited to a few privileged users from organizations such as Finance, Educational Aids, Student Records, and the



FLETC Information Management Officer. If a student user cannot remember his or her user ID or cannot answer the questions, they will be directed to one of these super users.

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

All users must have both annual privacy and IT Security training prior to receiving access to the system.

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

SASS 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 DHS Program Manager. These business decisions are documented in the SASS design documentation. Access to SASS falls in four general categories: (1) students; (2) SASS administrative users (e.g. training coordinators, training managers, instructors, etc.); (3) Partner Organization users; and (4) system administrators including database administrators, network engineers, etc.

Once they have been registered for training in SASS, the system generates an e-mail to the student that includes the student's login information. The SASS program office grants access to SASS 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. The SASS program office grants access to Partner Organization users at the request of the Partner Organization's Agency Representative to FLETC.

System administrators are responsible for the actual software and hardware that SASS operates on. Personnel having system level access to the SASS 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), Memorandums of Understanding, 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, Office of IT Budget, Policy, & Plans  
Federal Law Enforcement Training Center  
Department of Homeland Security

### **Approval Signature**

PIA signed and on file with the DHS Privacy Office.

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