1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: 27 July 2010

(b) Name of system: Student Training Management System

(c) System acronym: STMS

(d) IT Asset Baseline (ITAB) number: 303

(e) System description (Briefly describe scope, purpose, and major functions):

The purpose of STMS is to manage student registrations, enroll students into classes and document successful completions or scores. It also provides billing services for the budget office, records and tracks training of Department of State (DoS) and other agencies' personnel; tracks courses offered, registers students, scheduled classes, records test results, tracks skill sets, billing and produces a variety of training reports.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ **To update existing PIA to new format**

(g) Explanation of modification (if applicable): not applicable

(h) Date of previous PIA (if applicable): 5 May 2009

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system?

- Name;
- Email Address;
- DOB;
- SSN;
- Pay Plan;
- Grade;
- Employee ID;

- GEMS ID;
- FSN Payroll ID;
- Place of assignment;
- Phone numbers; and
- Billing information

b. What are the sources of the information?

The sources of information are:

- DoS employees and eligible family members
- Employees and eligible family members of other Government agencies
- DoS and other agencies' contractors
- Individuals from private sector business

c. How is the information collected?

STMS interfaces with Human Resources System and Global Employee Management System (GEMS). The employees' personal and position data is transferred to STMS on a daily basis. GEMS information is limited to DoS employees. Information from other Federal Agencies is obtained from their Personnel Office or the Training Officer via the SF-182 form. Contractor information is obtained via DS-755 (for DoS) or SF-182 (for non-DoS), from the individual or their Contracting Officer's Technical Representative. Information from individuals from private sector business is obtained via form DS-3083.

d. Why is the information collected and maintained?

Information is collected for enrollment into courses and to document the completion of the course.

All government agencies are mandated as part of the Enterprise Human Resources Integration (one of five OPM-led e-Government initiatives) to collect and submit training records (27 specific data fields), including Privacy Act information. The data fields are electronically transmitted by the Bureau of Human Resources to OPM to meet mandatory federal reporting requirements. Authorization for privacy act data to be collected is under: P.L. 79-724 (FS Act); P.L. 85-507 (GETA); and E.O. 9397 ("Numbering System for Federal Accounts Relating to Individual Persons" which authorizes agencies to ask for record subjects' SSN). Additionally, 5 USC 4115 allows the collection of training data and reporting through the form SF-182: "The Office of Personnel Management, to the extent it considers appropriate in the public interest, may collect information concerning training programs, plans, and the methods inside and outside the Government. The Office, on request, may make the information available to an agency and to Congress."

e. How will the information be checked for accuracy?

The individuals and personnel department of various agencies are responsible for verifying the students' data before submitting SF-182, DS-755 or DS 3083 to FSI. DoS data is validated with information in GEMS. FSI's Registrar Office oversees the quality of the data entered and modified in STMS.

f. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 USC 301; Federal Information

- 22 USC 4021

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

The information collected by STMS is the minimum amount required to meet the needs of FSI. There is minimal privacy risk associated with this system. The risk is identified as part of the annual information assurance testing of internal controls and processes. The risks are mitigated by limiting access to PII to only authorized users with need to know.

4. Uses of the Information

a. Describe all uses of the information.

The information will be used to determine a person's eligibility for enrollment, maintain student records and other administrative functions. The applicant's SSN will be used to distinguish his or her records from other students.

A student's first name, last name, email, and People Code ID will be provided to FSI ShareSites for automated student access management. (Note: the People Code ID is a unique system-generated ID associated with each student record that also serves as the key linking the system and its interfaces.) The email address will be used by the FSI ShareSites system to send alerts and other system messages to the student.

b. What types of methods are used to analyze the data?

There is no "analysis" of the information – it is solely used for the purposes stated above.

c. What new information may be produced?

None

d. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

None used; the system does not use commercial information, publicly available information, or information from other Federal agency databases.

e. Is the system a contractor used and owned system?

STMS is the property of the FSI and is ultimately owned by the DoS. However, contractors are involved with the design and development and use of STMS.

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

STMS performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, adequate safeguards are in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

5. Retention

a. How long is information retained?

FSI is in the process of creating an approved National Archive and Record Administration Disposition schedule. The recommended retention period to keep the data is 75 years.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The information is only retained for the amount of time that is required to perform the system's purpose. There are minimal risks with unauthorized use or exposure. The risks are mitigated by limiting access to the data only to those authorized through a formal approval process with the need to know.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

STMS receives data from the Department's Human Resource system, GEMS, including PII. FSI provides HR with training data only for the individuals whose information was originally transferred to STMS from GEMS. Therefore, no PII is shared with other bureaus within the Department.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Authorized users are granted access through a user account and login. Authorized users have roles assigned to them specific to their job function. All users must have access to OpenNet prior to access to STMS. Training data is provided to HR system through files daily. Authorized HR staff runs tasks that import the data into GEMS.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

User access is restricted. The network operating system access controls limit who can logon, what resources will be available, what each user can do with these resources, and where access is available. System managers, key security, and user personnel coordinate closely to implement access controls.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The information is shared with the Office of Personnel Management (OPM). All agencies are required by the Enterprise Human Resource Initiative (EHRI) to provide OPM with training data for all direct-hire employees.

b. How is the information shared outside the Department?

FSI provides the training data to HR, which in turn transmits the training data to OPM. HR provides the data electronically through a secure exchange process. HR

also provides an update when the data is transferred including the date of transfer and the count of records.

FSI provides USAID with a monthly file containing information on training completions by USAID employees. PII is limited to student name and government email addresses.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

FSI ensures the integrity and confidentiality of data provided to the Department's HR system, GEMS. Internal controls are in place for system access. Only authorized staff have access to PII.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

Foreign Service Institute Records – State 14

☐ does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Yes. Notice is available on forms that are completed by the individual and System of Records Notice State-14.

b. Do individuals have the opportunity and/or right to decline to provide information?

Providing the information is voluntary. However failure to provide the information may result in ineligibility of participation in the training program or error in processing training application.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Same as above

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

The notice given is adequate, and there are no risks associated.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals should follow the procedures in State-14, to amend information they believe to be incorrect.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notice is reasonable and adequate for this system.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access?

Internal access to STMS is limited to authorized DoS staff having a need for the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to STMS requires a unique user account. Criteria, procedures, controls, and responsibilities regarding access are all documented. All employees and contractors must follow the system behavior rules established by the Department.

b. What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The system maintains a system log of events as required by the Security Controls for a "Moderate" impact system. Reference pertinent C&A document for detailed Security Controls.

c. What privacy orientation or training for the system is provided authorized users?

Every DoS user must attend a security briefing prior to receiving access to DoS networks and getting a badge for facility access. This briefing includes the Privacy Act of 1974. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a DoS network.

d. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Minimal residual risk is anticipated.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

There are no technologies used in the system that involve privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Not applicable.

12. Security

What is the security certification and accreditation (C&A) status of the system?

STMS was authorized-to-Operate in July of 2010 via C& A Process. Thus, the authorization will expire in July of 2013.