Billing Code 4710-34

DEPARTMENT OF STATE

[Public Notice: 12067]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: The information contained within Foreign Service Institute (FSI or the "Institute") systems is used to provide the Institute's student information and training delivery management services to support the staff and students, and to facilitate billing services.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice is effective upon publication, except for routine uses (a) and (b) that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Questions can be submitted by mail, email, or by calling Eric F. Stein, the Senior Agency Official for Privacy, on (202) 485-2051. If mail, please write to: U.S Department of State; Office of Global Information Systems, A/GIS; Room 4534, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at Privacy@state.gov. Please write "Foreign Service Institute Records, State-14 " on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room 4534, 2201 C St., N.W.; Washington, DC 20520 or by calling (202) 485-2051.

SUPPLEMENTARY INFORMATION: This notice is being modified to reflect updated training delivery management services, the Department's move to cloud storage, new OMB guidance, access by contractors, and updated contact information. Specifically, the modified system of records notice includes substantive revisions and additions to the following sections: Summary, Dates, Supplementary Information, System Location, Purpose(s) of the Systems, Categories of Records in the Systems, Record Source Categories, Policies and Practices for Storage of Records, Policies and Practices for Retention and Disposal of Records, Policies and Practices for Retrieval of Records, Safeguards, Record Access Procedure, and History. It also includes minor administrative updates in the following sections: Addresses, For Further Information Contact, Categories of Individuals, Routine Uses, and Systems Manager.

SYSTEM NAME AND NUMBER: Foreign Service Institute Records, State-14.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: The George P. Shultz National Foreign Service Institute, 4000 Arlington Boulevard, Arlington, VA. Some records may be stored within U.S government authorized cloud-based systems that are FedRAMP certified and overseen by the Department's IRM Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEMS MANAGER(S): Executive Director for Management, Foreign Service Institute, SA-42, Room F- 2128, 4000 Arlington Blvd, Arlington, VA 22204, OMISwork@state.gov

AUTHORITY FOR MAINTENANCE OF THE SYSTEMS: 5 U.S.C. 301 (Management of Executive Agencies); 22 U.S.C. 4021-4029 (Chapter 7 of the Foreign Service Act of 1980).

PURPOSE(S) OF THE SYSTEM: The information contained within Foreign Service Institute (FSI) systems is used to provide the Institute's student information and training delivery management services, to support the staff and students, and for billing services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Persons who requested and/or received training from the Foreign Service Institute, took a language proficiency test given by the Foreign Service Institute, or received external training (including at colleges and universities) sponsored or approved by the Institute including, but not limited to: (1) employees (and eligible family members thereof) of the Department of State; (2) employees (and eligible family members thereof) of other federal agencies; (3) members (and eligible family members thereof) of the U.S. military; (4) citizens or nationals of the United States, or employees of any corporation, company, partnership, association or other legal entity that is 50 percent or more beneficially owned by citizens or nationals of the United States, that is engaged in business abroad, as well as immediate family members of such individuals; (5) citizens or nationals of the United States, or employees of any corporation, company, partnership, association or other legal entity that is 50 percent or more beneficially owned by citizens or nationals of the United

States, under contract to provide services to the United States Government or any employee thereof that is performing such services; and (6) applicants for employment at the Department of State. The Privacy Act defines an individual at 5 U.S.C. 552a(a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: Training request forms and supporting documentation; progress reports; evaluation reports; course grades and/or test scores; general correspondence; biographic information; educational and employment history; security clearance data; travel vouchers; fiscal, i.e., payment or billing, information.

RECORD SOURCE CATEGORIES: These records contain information that is primarily obtained from the individual who is the subject of the record.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Foreign Service Institute Records may be disclosed:

To appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(a.) To another Federal agency or Federal entity, when the Department of State

determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(b.) To other federal agencies that send students to the Institute for training.

(c.) To non-federal organizations that send students to the Institute for training.

(d.) To universities to which the Institute sends students for training.

(e.) To other training vendors to which the Institute sends students for training.

The Department of State periodically publishes in the Federal Register its standard routine uses that apply to all its Privacy Act systems of records. These notices as stated below appear in the form of a Prefatory Statement (published in Volume 73, Number 136, Public Notice 6290, on July 15, 2008). All these standard routine uses apply to Foreign Service Institute Records, State-14.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored both in hard copy and on electronic media. A description of standard Department of State policies concerning storage of electronic records is found at https://fam.state.gov/FAM/05FAM/05FAM0440.html. All hard copies of records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel only.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual name, the last four digits of Social Security Number, or other unique identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA) and outlined at https://foia.state.gov/Learn/RecordsDisposition.aspx. Digital records in FSI systems that are no longer active are updated with an inactive flag. They remain for 60 years after the inactive status is set. FSI follows the Department of State's e-Records disposition schedule when records are 100 years old. More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet users are required to take the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. Before being granted access to Foreign Service

Institute Records, a user must first be granted access to the Department of State computer system.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's mobile and remote access program and is limited to information maintained in unclassified information systems. Remote access to the Department's information systems is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records have undergone a thorough background security investigation. Access to the Department of State, its annexes, and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

The safeguards in the following paragraphs apply only to records that are maintained in government-certified cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Information that conforms with Department-specific definitions for Federal Information Security Modernization Act (FISMA) low, moderate, or high categorization

are permissible for cloud usage and must specifically be authorized by the Department's Cloud Program Management Office and the Department of State Authorizing Official. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, National Institute of Standards and Technology's (NIST) Special Publications (SP) and Federal Information Processing Standards (FIPS) and Department of State policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Department of State Authorizing Official. High FISMA impact risk level systems will additionally be subject to continual auditing and monitoring, multifactor authentication mechanism utilizing Public Key Infrastructure (PKI) and NIST 800 53 controls concerning virtualization, servers, storage, and networking, as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-

266; Washington, DC 20520. The individual must specify that he or she wishes the Foreign Service Institute Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that Foreign Service Institute Records include records pertaining to the individual. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at https://foia.state.gov/Request/Guide.aspx.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he/she wishes the Foreign Service Institute Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the

approximate dates) which gives the individual cause to believe that Foreign Service Institute of Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a (k)(6) records in this system of records may be exempted from 5 U.S.C. 552a(c)(3), (d), (e)(l), (e)(4)(G), (H) and (I) and (f).

HISTORY: Previously published at 71 FR 8882 (February 21, 2006).

Eric F. Stein,

Deputy Assistant Secretary,

Global Information Services (A/GIS),

Department of State.