POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

The records are stored in a database on magnetic disk and tape. A record, or any part thereof, may be printed and stored in the applicant's A-file.

RETRIEVABLITY:

Records are indexed and retrievable by name and/or A-file number.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

RETENTION AND DISPOSAL:

The following USCIS proposal for retention and disposal is pending approval by NARA:

Master File automated records will be maintained for 25 years after the case is closed, and then archived at the DOJ Data Processing Center or its designated successor, for 75 years and then destroyed. Copies of system data may be stored in the individual's Alien File (NCI–85–80–5/1).

Reports used to facilitate case processing that contains personally identifiable information will be maintained at Headquarters and Asylum Field Offices and destroyed when no longer needed.

SYSTEM MANAGER AND ADDRESS:

The Chief of the Asylum Division, Refugee, Asylum and International Operations Directorate, U.S. Citizenship and Immigration Services, Suite 3300, 20 Massachusetts Avenue, NW., Washington, DC 20529.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because of criminal, civil, and administrative enforcement requirements. However, USCIS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0655, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records are obtained from the individuals who are the subject of these records. Information contained in this system may also be supplied by DHS, other U.S. Federal, State, tribal, or local government agencies, foreign government agencies, and international organizations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 29, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–31267 Filed 1–4–10; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2009–0104]

Privacy Act of 1974; Department of Homeland Security U.S. Immigration and Customs Enforcement—001 Student and Exchange Visitor Information System (SEVIS) System of Records

AGENCY: Privacy Office, DHS.

ACTION: Modification to an existing system of records.

SUMMARY: The Department of Homeland Security U.S. Immigration and Customs Enforcement is modifying an existing system of records titled Student and Exchange Visitor Information System (Mar. 22, 2005), to reflect proposed changes in the personal information that will be collected and maintained on individuals. In conjunction with its development and launch of the next generation Student and Exchange Visitor Information System application, called Student and Exchange Visitor Information System II, U.S. Immigration and Customs Enforcement is modifying the Student and Exchange Visitor Information System system of records notice to propose the collection of additional information on students, exchange visitors, and their dependents who are in the U.S. on F, M, or J classes of admission (F/M/J nonimmigrants), and officials of approved schools for and designated sponsors of F/M/J nonimmigrants. Like its predecessor, Student and Exchange Visitor Information System II is an information system that tracks and monitors F/M/J nonimmigrants throughout the duration of approved participation within the U.S. education system or designated exchange visitor program. This Student

and Exchange Visitor Information System II system of records notice updates categories of individuals; categories of records; purpose of the system; routine uses; policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system; and record access procedures. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. A Privacy Impact Assessment on Student and Exchange Visitor Information System II that describes the new system in detail is being published concurrently with this notice.

DATES: Submit comments on or before February 4, 2010. This amended system will be effective February 4, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS–2009–0104 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.
- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided.
- *Docket:* For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions please contact: ITMB Chief, ICE Student and Exchange Visitor Program, 2450 Crystal Drive, Tower 1 9th Floor, Arlington, VA 22201, by telephone (703) 603–3400 or by facsimile (703) 603–3598. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to Section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104–208, 110 Stat. 3009, as amended, and other statutes, Congress mandated that the Department of Homeland Security (DHS) in consultation with the Department of State (DOS) develop a national system to collect and maintain pertinent information on nonimmigrant students, exchange visitors, and their dependents admitted to the U.S. under an F, M, or J class of admission (F/M/J nonimmigrants), and the schools and exchange visitor program sponsors that host these individuals in the United States. In accordance with that mandate the Immigration and Naturalization Service, the predecessor to U.S. Immigration and Customs Enforcement (ICE), developed the Student and Exchange Visitor Information System (SEVIS) and deployed the system in January 2003. In 2005, after SEVIS was transferred to ICE, DHS published a system of records notice (SORN) titled DHS/ICE–001, Student and Exchange Visitor Information System, (70 FR 14477, Mar. 22, 2005), and a PIA that described the SEVIS application and data.

Currently, ICE is developing the next generation SEVIS system, called SEVIS II, which will serve the same purpose and provide the same capabilities as the original system, plus additional features such as user accounts for F/M/J nonimmigrants. SEVIS II will deploy in two phases; the first phase will occur in early 2010 and will allow SEVIS II users, such as students, exchange visitors, schools and sponsors, to establish their SEVIS II customer accounts on a voluntary basis. The personal data collected from individuals during the first phase is limited to user account data. The first phase will also support the periodic migration of SEVIS data to SEVIS II. During the first phase, users that elect to establish SEVIS II accounts may view their migrated record and request correction of any incorrect information. The original SEVIS system will remain operational during the first phase.

The second and final phase of SEVIS II deployment will occur at a date yet to be determined. This phase will implement all other SEVIS II functionality as described in this PIA and SEVIS II will become the system of record in which all student and exchange visitor transactions described in this PIA will occur. With the full deployment of SEVIS II, ICE will migrate all data from and retire the original SEVIS system. ICE will retain a copy of the original SEVIS dataset separate from SEVIS II for seven (7) years in case it is needed for reference or to repopulate the SEVIS II system if a problem is identified with the data migration.

DHS is updating this notice to include the following substantive changes: (1) An update to the categories of individuals to include perspective and former nonimmigrants and their dependents to the U.S. on a F, M, or J class of admission; (2) categories of records to include the addition of SEVIS II account requirements; (3) purpose of the system to include the ability to identify and act on potential violations by schools, sponsors, and F, M, or J nonimmigrants; (4) several routine uses were updated to reflect the standard DHS routine uses; (5) the addition of routine uses to (a) permit disclosure of SEVIS data to relevant parties in litigation, including the courts, parties, opposing counsel and witnesses, (b) provide for other litigation disclosures, including during the course of settlement negotiations, (c) allow to disclose information to foreign governments about their citizens or permanent residents during a disaster or health emergency, (d) allow SEVIS to verify an F/M/J nonimmigrant's information when payment is made, and ensure it is credited to the right person, (e) allow Student and Exchange Visitors Program and schools/sponsors to exchange data to assist in the functions necessary to process and monitor individuals in the program, (f) allow for disclosure of SEVIS data to the DOS's Consolidated Consular Database (CCD) for use by consular officers and other CCD users, (g) support sharing with government agencies for the research and development software and technologies to the Student and Exchange Visitor Program; and (6) policies and practices for storing retrieving, accessing, retaining, and disposing of records in the system.

The new SEVIS II system will maintain personal information on officials of approved schools and designated sponsors that host F/M/J nonimmigrant students and exchange visitors. It also will maintain personal information on F/M/J nonimmigrants. The personal information collected under SEVIS II will be somewhat different than under the original SEVIS system. New personal data elements will be collected from F/M/J nonimmigrants and school/exchange visitor sponsor officials; the new data will primarily be used to establish SEVIS II user accounts for these individuals. In addition, limited personal information that was collected and maintained in the original SEVIS system will not be used by SEVIS II and therefore will not be migrated to the new system (i.e., Social Security Numbers, driver's license information).

In accordance with the Privacy Act of 1974 (Privacy Act), 5 U.S.C. 552a, the DHS is amending DHS/ICE–001, Student and Exchange Visitor Information System (SEVIS) SORN, to reflect changes in the personal information that will be maintained

with the deployment of SEVIS II. This amended system of records supports ICE's mandate to track and monitor F/M/J nonimmigrants throughout the duration of approved participation within the U.S. education system or designated exchange visitor program. The collection and maintenance of the information described in this amended SORN assists ICE and DOS's Bureau of Educational and Cultural Affairs in meeting their obligations and legislative mandate. This amended SORN is being published concurrently with the SEVIS II PIA. Pursuant to the final rule that exempts the SEVIS SORN from certain requirements of the Privacy Act (73 FR 63057, Oct. 23, 2008), portions or all of these records may be exempt from disclosure pursuant to 5 U.S.C. 552a(k)(2).

Consistent with DHS's information sharing mission, information stored in SEVIS II may be shared with other DHS components, as well as appropriate Federal, State, local, Tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this SORN.

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of DHS/ICE–001, Student and Exchange Visitor Information System (SEVIS) system of records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

System of Records DHS/ICE–001

SYSTEM NAME:

Student and Exchange Visitor Information System (SEVIS).

SECURITY CLASSIFICATION:

Unclassified, sensitive.

SYSTEM LOCATION:

Records in the SEVIS II application are maintained in electronic form in a government-secured facility located in Rockville, Maryland and at a contingency site.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: (1) Prospective, current and former nonimmigrants to the U.S. on an F–1, M–1, or J–1 class of admission and their dependents who have been admitted under an F–2, M–2, or J–2 class of admission (collectively, F/M/J nonimmigrants); (2) a proxy, parent or guardian of an F/M/J nonimmigrant; and (3) officials, owners, chief executives, and legal counsel of Student and Exchange Visitor Program (SEVP)-certified schools and designated exchange visitor sponsors.

F nonimmigrants are foreign students pursuing a full course of study in a college, university, seminary, conservatory, academic high school, private elementary school, other academic institution, or language training program in the U.S. that SEVP has certified to enroll foreign students. M nonimmigrants are foreign students pursuing a full course of study in a vocational or other recognized nonacademic institution (e.g., technical school) in the U.S. that SEVP has certified to enroll foreign students. J nonimmigrants are foreign nationals selected by a sponsor that the Department of State (DOS) has designated to participate in an exchange visitor program in the U.S.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

Biographical information for F/M/J nonimmigrants and school/sponsor officials used in the creation of SEVIS II user accounts, specifically names; U.S. domestic address; foreign address (F/M/J nonimmigrants only); date of birth; birth country and city; country of citizenship; country of legal permanent residence; username; e-mail addresses; the DHS-assigned Immigrant Identification Number (IIN); Alien Registration Number (A–Number) (for school/sponsor officials who are U.S. lawful permanent residents only); National Identity Number (for F/M/J nonimmigrants only); and passport information (number, issuing country, expiration date). This information would also be collected for any proxy, parent or guardian for an F/M/J nonimmigrant who is unable to create their own account due to age (under 13 years old), disability, or other reasons. The proxy, parent, or guardian would first need to create their own SEVIS II account before they could create an account for the F/M/J nonimmigrant.

F–1, M–1, or J–1 nonimmigrant educational and financial information, specifically program of study; school registration information; program completion or termination information; transfer information; leave of absence information and study abroad; extensions; change of education level; student ID number; I–901 fee payment information; and financial information (for F/M nonimmigrants, financial information includes data on source of funds—personal or school, and average annual cost—tuition, books, fees, and living expenses; for J nonimmigrants financial information includes total estimated financial support, financial organization name and support amount).

F/M/J nonimmigrant status and benefit information, specifically the DHS-assigned Fingerprint Identification Number (for individuals 14 years of age and older); U.S. visa number, issuing country, expiration date; class of admission; immigrant benefit application information (primarily reinstatement, employment authorization, 212e waiver, *etc.*); and arrival and departure information (port of entry, date of entry/exit).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Public Law 104–208, Illegal Immigration Reform and Immigrant Responsibility Act of 1996; Public Law 106–215, Immigration and Naturalization Service Data Management Improvement Act of 2000;

Public Law 106–396, Visa Waiver Permanent Program Act of 2000; Public Law 107–56, USA PATRIOT Act; and Public Law 107–173, Enhanced Border Security and Visa Entry Reform Act of 2002. The collection of information is mandated by 8 CFR 214.2 (f), (j), (m), 8 CFR 214.3, 8 CFR 214.4, and 22 CFR part 62.

PURPOSE(S):

The purpose of this system of records is to track F, M and J nonimmigrants and their dependents during their stay in the U.S. This system allows DHS and DOS to administer the student and exchange visitor programs by certifying and designating schools and sponsors and ensuring their ongoing compliance with Federal requirements and regulations. The system also enables DHS and DOS to monitor the progress and status of lawfully admitted F/M/J nonimmigrants residing in the United States, to ensure they comply with the obligations of their U.S. admittance, and to maintain a history of their status-related activities. The system is used to identify and act on potential compliance violations by schools, sponsors, and F/M/J nonimmigrants. The system is also used to support other homeland security and immigration activities, such as deciding F/M/J nonimmigrants' requests for immigration benefits and for admission to the U.S. Finally, the system supports the analysis of information in the system for law enforcement, reporting, management, and other mission-related purposes.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (1) DHS or any component thereof; (2) any employee of DHS in his/her official capacity; (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or (4) the United States or any agency thereof; is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, Tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

I. To a court, magistrate, administrative tribunal, opposing counsel, parties, and witnesses, in the course of a civil or criminal proceeding before a court or adjudicative body when (a) DHS or any component thereof; or (b) any employee of DHS in his or her official capacity; or (c) any employee of DHS in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States, where DHS determines that litigation is likely to affect DHS or any of its components, is a party to litigation or has an interest in such litigation, and DHS determines that use of such records is relevant and necessary to the litigation, provided however that in each case, DHS determines that disclosure of the information to the recipient is a use of the information that is compatible with the purpose for which it was collected.

J. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings.

K. To an attorney or representative who is acting on behalf of an individual covered by this system of records for use in any proceeding before the Executive office for Immigration Review.

L. To clerks and judges of courts exercising naturalization jurisdiction for the purpose of filing petitions for naturalization and to enable such courts to determine eligibility for naturalization or grounds for revocation of naturalization.

M. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant

public health threats; appropriate notice will be provided of any identified health threat or risk.

N. To foreign governments for the purpose of providing information about their citizens or permanent residents, or family members thereof, during local or national disasters or health emergencies.

O. To the U.S. Treasury Department and its contractors for the purpose of facilitating and tracking Student and Exchange Visitor Program fee payments made by F/M/J nonimmigrants.

P. To certified schools and designated exchange visitor sponsors participating in the Student and Exchange Visitor Program for the purpose of certification and designation, enrollment and monitoring of F/M/J nonimmigrants, audit, oversight, and compliance enforcement.

Q. To the U.S. Department of State for the purpose of visa issuance to F/M/J nonimmigrants; the operation of its Exchange Visitor Program; or the enforcement of and investigation into its visa and Exchange Visitor Program laws, regulations, and requirements.

R. To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

S. To appropriate Federal, State, local, Tribal, or foreign governmental agencies or multilateral governmental organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems for SEVIS II or other systems supporting the Student and Exchange Visitor Program.

T. To appropriate Federal, State, local, Tribal, or foreign government agencies or multinational government organizations where DHS desires to exchange relevant data for the purpose of developing new software or implementing new technologies for the purposes of data sharing to enhance the efficiency of the Student and Exchange Visitor Program or homeland security.

U. To a Federal, State, Tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

V. To a former employee of the Department for purposes of: responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

W. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

X. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by Immigration Identification Number, name and school, name and citizenship country, name and entry detail, name and date of birth, and passport number.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RETENTION AND DISPOSAL:

Inputs will be deleted after the data has been transferred to the master file and verified. The master file will be retained for 75 years. System outputs are deleted or destroyed when no longer needed for agency business. Once SEVIS II terminates a non-government SEVIS II user account, the system retains user information for 75 years from the date of last transaction. Government user audit information will be retained for seven years. At this time, SEVP envisions destroying their SEVIS audit records seven years after the date SEVIS II is fully operational. The data from the legacy SEVIS will be retained for seven (7) years.

SYSTEM MANAGER AND ADDRESS:

ITMB Chief, ICE Student and Exchange Visitor Program, 2450 Crystal Drive, Tower 1 9th Floor, Arlington, VA 22201.

NOTIFICATION PROCEDURE:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, ICE will consider requests to determine whether or not information may be released. Thus, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under ''contacts.'' If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP–0550, Washington, DC 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity,

meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Director, Disclosure and FOIA, *http://www.dhs.gov* or 1–866–431–0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records are obtained directly from individuals who create a SEVIS II account (F/M/J nonimmigrants; parents, proxies and guardians; and school and sponsor officials, owners, chief executives, and legal counsel. Status information about F/M/J nonimmigrants is also obtained from schools and sponsors. Records are also obtained from other Federal agency information systems, including the DHS Arrival and Departure Information System (ADIS); the DHS Automated Biometric Identification System (IDENT); U.S. Treasury Department's I–901 Web portal; DOS's Consular Consolidated Database (CCD); and USCIS's Computer-Linked Application Information Management System 3 Mainframe (CLAIMS 3).

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Certain portions or all of these records may be exempt from disclosure pursuant to 5 U.S.C. 552a(k)(2).

The Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G) and (H), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

Dated: December 29, 2009.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E9–31268 Filed 1–4–10; 8:45 am]

BILLING CODE 9111–28–P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Statewide Communication Interoperability Plan Implementation Report

AGENCY: National Protection and Programs Directorate, Department of Homeland Security.

ACTION: 60-Day Notice and request for comments; New Information Collection Request: 1670–NEW.

SUMMARY: The Department of Homeland Security, National Protection and Programs Directorate/Cybersecurity and Communications/Office of Emergency Communications, has submitted the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. Chapter 35).

DATES: Comments are encouraged and will be accepted until March 8, 2010. This process is conducted in accordance with 5 CFR 1320.1.

ADDRESSES: Written comments and questions about this Information Collection Request should be forwarded to NPPD/CS&C/OEC, Attn.: Jonathan Clinton, *Jonathan.Clinton@dhs.gov.*

SUPPLEMENTARY INFORMATION: The Office of Emergency Communications (OEC), formed under Title XVIII of the Homeland Security Act of 2002, 6 U.S.C. 101 *et seq.,* is responsible for ensuring that activities funded by the Interoperable Emergency Communications Grant Program (IECGP) (6 U.S.C. 579) comply with the Statewide Communication Interoperability Plan (SCIP) for that State required by section 7303(f) of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194(f)). Further, under the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 579(m)), a State that receives a grant under the IECGP must annually submit to the Director of OEC a report on the progress of the State in implementing its SCIP and on achieving interoperability at the city, county, regional, State, and interstate levels. OEC is then required to make these reports publicly available (6 U.S.C. 579(m)). The SCIP Implementation Report Form is designed to meet these statutory requirements. SCIP Implementation Reports will be submitted electronically.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate.

Title: Statewide Communication Interoperability Plan Implementation Report.

Form: Not Applicable.

OMB Number: 1670–NEW.

Frequency: Yearly.

Affected Public: State, local, or tribal government.

Number of Respondents: 56.

Estimated Time per Respondent: 6 hours.

Total Burden Hours: 336 annual burden hours.

Total Burden Cost (operating/maintaining): $8,205.12.

Signed: December 22, 2009.

Thomas Chase Garwood, III,

Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. E9–31266 Filed 1–4–10; 8:45 am]

BILLING CODE 9910–9P–P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2009–1100]

Certificate of Alternative Compliance for the High Speed Ferry SUSITNA

AGENCY: Coast Guard, DHS.

ACTION: Notice.

SUMMARY: The Coast Guard announces that a Certificate of Alternative Compliance was issued for the high speed ferry SUSITNA as required by 33 U.S.C. 1605(c) and 33 CFR 81.18.

DATES: The Certificate of Alternative Compliance was issued on December 18, 2009.

ADDRESSES: The docket for this notice is available for inspection or copying at the Docket Management Facility (M–30), U.S. Department of Transportation,