



Privacy Impact Assessment
for the

Student & Exchange Visitor Information System II

December 4, 2009

Contact Point

James Dinkins

Director, Office of Investigations

U.S. Immigration and Customs Enforcement

(202) 732-5100

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

(703) 235-0780



Abstract

The Department of Homeland Security U.S. Immigration and Customs Enforcement (ICE) is developing the Student & Exchange Visitor Information System II (SEVIS II) as a modernization effort to address limitations in the original SEVIS immigration benefits tracking tool. SEVIS II is an information system that tracks and monitors students, exchange visitors, and their dependents that are in the U.S. on F, M, or J classes of admission throughout the duration of approved participation within the U.S. education system or designated exchange visitor program. SEVIS also maintains information on the schools, exchange visitor program sponsors, and their representatives. ICE is conducting this Privacy Impact Assessment (PIA) to document publicly the privacy protections that are in place within the system because SEVIS II collects, maintains, and provides personally identifiable information (PII) in the execution of its mission. SEVIS II will be deployed in two phases; however this PIA describes the system as it will be fully deployed.

Overview

The Student and Exchange Visitor Program (SEVP), a division of the ICE Office of Investigations, owns SEVIS II. SEVIS II supports the application and admission of foreign nationals who seek to come to the U.S. as students and exchange visitors under F, M, or J classes of admission. SEVIS II maintains PII about these foreign nationals and any dependents that come with them to the U.S. In addition, SEVIS II maintains PII about officials of approved schools and designated exchange visitor program sponsors as well as American families who host nonimmigrant students and exchange visitors.

SEVIS II will deploy in two phases; the first phase will likely occur in 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 (described in Question 1.1). 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.

Background

The U.S. has a history of welcoming foreign nationals into our country as students or exchange visitors. While they stay for an extended period, the U.S. considers them nonimmigrant, temporary visitors.

When nonimmigrants apply for admission to the U.S., they must declare their primary purpose for visiting. Based upon that purpose, U.S. immigration law recognizes a number of classes of admission,



such as those for tourists and business travelers. For foreign students and exchange visitors, the U.S. immigration law recognizes the following three classes of admission:

- **F-1 Admission:** For foreign students pursuing a full course of study in a college, university, seminary, conservatory, academic high school, private elementary school, or other academic institution or language training program in the U.S. that SEVP has certified to enroll foreign students.
- **M-1 Admission:** For foreign students pursuing a full course of study in a U.S. vocational or other recognized nonacademic institution (e.g., technical school) that SEVP has certified to enroll foreign students.
- **J-1 Admission:** Foreign nationals who are selected by a Department of State (DOS)-designated Exchange Visitor Program sponsor to participate in an exchange visitor program in the U.S.¹

F-1, M-1, and J-1 nonimmigrants may bring their eligible spouse and dependent children (hereafter, dependents) with them for the duration of their stay. Dependents of F-1, M-1, or J-1 nonimmigrants are admitted to the U.S. under a corresponding class of admission: F-2, M-2, or J-2. Their purpose for visiting is to accompany or are following to join the F-1, M-1, or J-1 nonimmigrant (the principal nonimmigrant for the family). Dependents may stay only as long as the principal nonimmigrant maintains legal immigration status.

A foreign national who wishes to come to the U.S. as a foreign student or exchange visitor on an F-1, M-1, or J-1 class of admission must do all of the following:

- Apply to and be accepted by an SEVP-certified school or a DOS-designated Exchange Visitor Program sponsor.
- Obtain a student or exchange visitor visa from an embassy or consulate abroad or, if from a visa exempt country (e.g., Canada or Bermuda), apply for admittance at a U.S. port of entry (POE), or if already in the United States in another nonimmigrant class of admission, obtain a change of status to F, M, or J from U.S. Citizenship and Immigration Services (USCIS).

In addition, F and M nonimmigrants must be able to pay the cost of schooling and living expenses while in the U.S. and furnish proof of sufficient funding to the school.

F/M/J nonimmigrants must comply with federal regulations that are specific to their class of admission. These regulations dictate eligibility requirements, required activities, and prohibited activities. F/M/J nonimmigrants who do not continue to comply with these requirements are “out of status,” and they and their dependents cannot remain in the U.S.

The Student and Exchange Visitor Program and the Office of Private Sector Exchange

¹ The DOS Exchange Visitor Program is an international exchange program that implements the Mutual Educational and Cultural Exchange Act of 1961, as amended, by means of educational and cultural exchanges. The purpose of the Program is to provide foreign nationals with opportunities to participate in educational and cultural programs in the United States and return home to share their experiences, and to encourage Americans to participate in educational and cultural programs in other countries. Exchange visitor programs vary and include au pairs, professors, and trainees in various occupational categories.



Two separate federal offices work collaboratively on issues involving the regulation of the student and exchange visitor process in the U.S. Those offices are ICE's SEVP and DOS's Office of Private Sector Exchange (OPSE) in the Bureau of Educational and Cultural Affairs.

ICE's SEVP is responsible for certifying academic and technical schools in the U.S. that seek to bring F or M nonimmigrants to study at their school. SEVP determines if the school meets the regulatory requirements for certification. The schools designate officials who are responsible for updating SEVIS II (and previously, SEVIS) with current school-related information on F and M students. SEVP also monitors certified schools to ensure compliance with reporting and recordkeeping requirements. SEVP has an intensive outreach program to ensure that school officials have the information and training to comply with all requirements. In addition, SEVP manages the fees collected from F/M/J nonimmigrants. It also manages and operates SEVIS II and is responsible for maintaining and updating the section of federal regulations dealing with Aliens and Nationality (Title 8, Code of Federal Regulations) that pertain to F/M/J nonimmigrants and SEVP-certified schools.

DOS's OPSE administers the Exchange Visitor Program, which governs the allowed activities of nonimmigrants in the J class of admission. OPSE designates an Exchange Visitor Program applicant to conduct an Exchange Visitor Program as a sponsor and determines which categories of exchange visitors they may sponsor. OPSE also monitors the compliance of sponsors with DOS regulations and DHS regulations on immigration. OPSE works closely with SEVP in the ongoing development of SEVIS II capabilities.

The Student and Exchange Visitor Information System

Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) in 1996 (Public Law 104-208) that authorized the former Immigration and Naturalization Service (INS) to create an electronic system to collect information on F/M/J nonimmigrants. The system was to support INS efforts to determine how many F/M/J nonimmigrants² are in the country, where they are, and what they are studying. After September 11, 2001, Congress updated the legislation mandating the use of an electronic system to collect information on all F/M/J nonimmigrants.

To meet this mandate, the Department of Homeland Security (DHS) and the DOS developed SEVIS, which deployed in January 2003. DHS published a PIA for SEVIS on February 5, 2005. SEVIS is a web-based information system that tracks and monitors F/M/J nonimmigrants and dependents throughout the duration of approved participation within the U.S. education system or designated exchange visitor program. SEVIS maintains records on these nonimmigrants and receives updated information from schools and sponsors, such as change of domestic address and changes in program study. SEVIS also maintains information on the schools, exchange visitor program sponsors, and their representatives.

Creation of SEVIS II

² SEVIS II does not track all cultural exchange visitors and all foreign students; it tracks **only** nonimmigrants admitted under F/M/J classes of admission. In some cases, nonimmigrants who are students or exchange visitors are in the U.S. on other classes of admission. As such, this PIA will use the term "F/M/J nonimmigrant" rather than the terms *foreign students and exchange visitor* to avoid confusion.



SEVIS II is a modernization effort to address limitations in the original SEVIS application. SEVIS II improves on the existing system in several areas. First, SEVIS II creates an entirely paperless process for all activities related to the admission and tracking of F/M/J nonimmigrants. Under SEVIS II, F/M/J nonimmigrants, school, and sponsor officials will use digital signatures to sign electronic forms related to the student and exchange visitor process. Government officials will also use SEVIS II—or a system that links to SEVIS II—to document electronically decisions about visa issuance, changes of status, entry into the U.S., and other requests for nonimmigrant benefits (e.g., employment authorization).

Second, SEVIS II permits F/M/J nonimmigrants to create user accounts and directly access their own information in the system. This feature of SEVIS II permits F/M/J nonimmigrants to view information about their status, immigration benefits, and payment of SEVP fees. F/M/J nonimmigrants will also be able to view their own information in the system in real time and request that SEVP make a change if it is inaccurate.

Third, SEVIS II creates a new, person-centric recordkeeping system that will unify information about the same F/M/J nonimmigrants that the original SEVIS maintained in multiple records. SEVIS II seeks to unify records about the same individuals by using immigration identification numbers (IINs) assigned to F/M/J nonimmigrants through the activation of SEVIS II accounts. SEVIS II also obtains the Fingerprint Identification Number for F/M/J nonimmigrants from the DHS's U.S. Visitor and Immigrant Status Indicator Technology's (US-VISIT's) Automated Biometric Identification System (IDENT). The Fingerprint Identification Number is an assigned numeric identifier linked to the F/M/J nonimmigrant's fingerprints, which are collected as part of the visa application process and/or upon admission to the U.S. SEVIS II uses the Fingerprint Identification Number to maintain the one-person, one-record system; however, SEVIS II does not collect, store, or process actual fingerprints or other biometric information.

Fourth, SEVIS II generates and displays an admissibility indicator for each F/M/J nonimmigrant that reflects whether they are currently eligible for admission into the U.S. under the terms of their F/M/J class of admission. F/M/J nonimmigrants may view their admissibility indicator in SEVIS II before traveling to the U.S. to confirm that they are eligible to enter the U.S. at that time. To generate the admissibility indicator, SEVIS II uses the information already in the system and a set of business rules to determine if the individual is currently eligible to enter the U.S. as an F/M/J nonimmigrant. SEVIS II exports the admissibility indicator to the U.S. Customs and Border Protection (CBP) TECS system to allow CBP officers to view the admissibility indicator when the F/M/J nonimmigrant arrives at the border and requests admission. The CBP officer uses the admissibility indicator as one factor in determining if the individual may enter as an F/M/J.

Finally, SEVIS II indicates whether a nonimmigrant is eligible for employment in the U.S. under the terms of his or her F/M/J class of admission. USCIS's E-Verify system queries SEVIS II in response to a request for an employment authorization.³ SEVIS II uses information already in the system and a set of business rules to determine if the nonimmigrant is eligible for employment, the maximum allowable length of employment, and (if applicable) the allowable location for employment under the terms of his or her F/M/J admission. This information is sent to E-Verify.

³ E-Verify is an Internet-based system operated by USCIS in partnership with the Social Security Administration that allows participating employers to electronically verify the employment eligibility of their newly hired



SEVIS II Users

There are three categories of SEVIS II users. The first category is comprised of F/M/J nonimmigrants and persons serving as proxies or parents/guardians. These users must have a customer account and an IIN. F/M/J nonimmigrants can view any pending request for benefits, initiate requests for certain actions from their school or sponsor officials, request corrections of data that appears incorrect, determine whether they are eligible to travel and enter/re-enter the U.S., view fee payment information, and determine whether SEVIS II indicates they are in or out of F/M/J status. Dependents may elect to either create their own SEVIS II accounts or allow the principal nonimmigrant to manage the process on behalf of the entire family; however, anyone over the age of 14 will be required to access their account in order to electronically sign their SEVIS II record. In certain circumstances, a proxy, parent, or guardian may create and maintain the SEVIS II account for select F/M/J nonimmigrants that are under the age of 14 or are unable to access SEVIS II.

The second category of SEVIS II users represent the schools and sponsors. These users must have a customer account and an IIN. Schools and sponsors initially use SEVIS II to apply for certification or designation that will allow them to enroll or sponsor F/M/J nonimmigrants. In SEVIS II, they enter information that government officials use to make the certification or designation decision. After certification or designation, selected employees become the designated or responsible officials. These employees must be U.S. citizens or lawful permanent residents of the United States. They use SEVIS II to update school and sponsor information, input information on F/M/J nonimmigrant applicants, and record information on events that relate to a nonimmigrant's status, such as enrollment, failure to enroll in a full course of study, failure to report to a program, or completion of a course of study or program. They can also recommend approval for status-related benefits (e.g., employment, transfers, and extensions of status).

The third category of SEVIS II users are select government agency employees who directly access SEVIS II through a user account rather than a customer account. Personnel at three agencies have direct access to SEVIS II through user accounts: DHS, DOS, and Department of Justice's (DOJ's) Federal Bureau of Investigation (FBI). DHS users are personnel working for ICE SEVP, who use SEVIS II to decide whether to certify a school to admit F or M nonimmigrants to a full course of study, to monitor the compliance of certified schools, to respond to questions about selected nonimmigrants, make determinations on requests for corrections, and to manage SEVIS II. DOS OPSE users access SEVIS II to determine whether to designate an entity as a sponsor in the Exchange Visitor Program. Both SEVP and OPSE personnel use SEVIS II in support of help desk services. Finally, FBI users access SEVIS II for information critical to criminal and intelligence investigations.

SEVIS II Information Sharing

SEVIS II is the system of record for information on schools, sponsors, and F/M/J nonimmigrants. When other federal offices and agencies need this information to carry out their missions, SEVIS II is the source. For example, extracts of SEVIS II data are shared with ICE's Office of Investigations, Compliance Enforcement Unit (CEU) to support CEU investigations into violations of immigration law and possible criminal activity of nonimmigrants. SEVIS II data is sent to USCIS to allow USCIS

employees.



personnel access to the information to support adjudication of immigration-related benefits and verify status and employment eligibility. SEVIS II data is also sent to CBP systems to allow its personnel to make decisions on eligibility for admission to the U.S. Outside of DHS, SEVIS II data is sent to a DOS Consular Affairs system to allow consular officials to use it in support of visa issuance decisions. SEVIS II extracts are also sent to the FBI’s Foreign Terrorist Tracking Task Force (FTTTF), which uses it for criminal and intelligence investigations. DHS also shares information from SEVIS II about individuals that meet specified homeland security threat criteria, who may require further investigation.

Section 1.0 Characterization of the Information

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

SEVIS II maintains information about F/M/J nonimmigrants and their dependents, SEVP-approved schools and school officials, and Exchange Visitor Program sponsors and sponsor officials. Table 1 below details exact data collected for each of these categories of information in the system. SEVIS II also contains address and family name information for American host families of au pairs and high school exchange visitors in order to monitor Exchange Visitor Program sponsor compliance with regulatory requirements.

Table 1: Information Category and Collected PII

Category of Information	Personally Identifiable Information Collected
Non-Government SEVIS II User Account Information (For all F/M/J nonimmigrants that create user accounts; and school and sponsor officials, owners, chief executives, legal counsel and/or proxies, parents, or guardians.)	<ul style="list-style-type: none"> -Name (first, middle, last) -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 -Immigrant Identification Number (IIN) -Alien Number (If the school or sponsor officials select U.S. as their legal permanent residence country but not the country of citizenship, then an Alien Number is required) -National Identity Number (identity number issued by foreign national’s home country. Requested from all F/M/J nonimmigrants, required for South Korean nationals) -Passport – optional (number, issuing country, expiration date)
F/M/J Principal Nonimmigrant Educational and Financial Information (For F-1, M-1, and J-1 nonimmigrants only)	<ul style="list-style-type: none"> -Program of study – educational level and first major, second major, and minor) -School Registration Information (major, course and registration information, program completion information, drop below full course information) - Exchange visitor program information (category, site of activity,



Category of Information	Personally Identifiable Information Collected
	program completion information) -Program completion or termination information -Transfer information -Out of country absences and study abroad -Extensions -Change of Educational Level -Student ID Number (number issued by U.S. school, optional, F/M only) - I-901 Fee Payment Information -Financial Information (For F and 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 (For all F/M/J Nonimmigrants, including dependents)	-Fingerprint Identification Number -Visa (number, issuing country, expiration date) -Class of admission -Immigrant benefit application information - (Primarily reinstatement, and employment authorization and 212(e) Waiver, etc.) -Arrival and departure information (POE and date of entry/exit) - Flag identifying individuals that meet specified homeland security threat criteria who may require further investigation

SEVIS II produces compliance monitoring reports and user-generated reports containing status and school/sponsor information for government and school/sponsor SEVIS II users only. The system also generates the admissibility indicator for F/M/J nonimmigrants by applying business rules to information already in the system. The admissibility indicator displays if the nonimmigrant is currently eligible to enter the U.S. (green), not eligible for entry (red), or may be eligible (yellow). F/M/J nonimmigrants can see this indicator in SEVIS II and CBP officers can view it through TECS.

The system also generates an employment eligibility determination for F/M/J nonimmigrants by applying business rules to information already in the system. USCIS’s E-Verify system queries SEVIS II for employment eligibility data on a particular nonimmigrant. SEVIS II sends in return the employment eligibility determination that reflects whether an F/M/J nonimmigrant is eligible to work in the U.S., the length of employment eligibility, and whether it is authorized for multiple employers.

1.2 What are the sources of the information in the system?

Most F/M/J principal nonimmigrant user account, educational and financial information (described in Table 1 above) is collected directly from the F/M/J principal nonimmigrant. In many cases, the F/M/J principal nonimmigrant will create, access, and maintain SEVIS II accounts for all dependents and will therefore serve as the source of information about them. Dependents may also elect to create their own username and password to gain access and control their account, and may serve as the source of certain biographic information about them in the system. See Question 1.1, Table 1 above, “Non-Government SEVIS II User Account Information.” A proxy, parent, or guardian may create a SEVIS II account for an F/M/J principal nonimmigrant who is under the age of 14 or is unable to access SEVIS II



due to a disability or other reasons. If the F/M/J principal nonimmigrant is under the age of 13, a parent or guardian must create their own account first to create an account for an F/M/J nonimmigrant.

SEVIS II also receives the following information on F/M/J nonimmigrants from sources other than the individual:

- The DHS Arrival and Departure Information System (ADIS) provides arrival and departure information on F/M/J nonimmigrants. ADIS is a repository of information from various systems on pre-entry, entry, status management, and exit of immigrants and nonimmigrants.
- The DHS US-VISIT IDENT system provides the Fingerprint Identification Number.
- Schools and sponsors provide information about enrollment or participation, programs of study, transfers, and detailed education and financial information on F/M/J nonimmigrants.
- The U.S. Treasury Department's I-901 web portal provides information about F/M/J nonimmigrants' payment of fees related to the SEVP. Nonimmigrants must use the I-901 payment website to pay fees to ICE related to the SEVP.
- The DOS Consular Consolidated Database (CCD) provides visa issuance information, corrected biographic information, and 212(e) waiver information. U.S. consular officials collect biographic information from F/M/J nonimmigrants during the visa issuance process and input it into CCD. Visa issuance information pertains to whether the DOS has issued or denied a visa to an F/M/J nonimmigrant. The DOS also collects information from J nonimmigrants applying for a waiver of the two-year foreign residency requirement through the completion of the 212(e) Waiver.
- The USCIS Computer-Linked Application Information Management System 3 (CLAIMS 3) provides information on USCIS's adjudication of immigration benefits sought by an F/M/J nonimmigrant.

Information about SEVIS II users who work for schools and sponsors is collected directly from those individuals during the user account registration and update processes.

The legacy SEVIS database is also a source of information in SEVIS II. Prior to the deployment of SEVIS II, ICE identified and merged SEVIS records about the same F/M/J nonimmigrants, schools, sponsors, and school and sponsor officials into a single SEVIS II record. These records were loaded into SEVIS II. In addition, SEVIS II uses commercial software to access U.S. Post Office address information to verify domestic addresses in the system.

SEVIS II itself is the source of user audit data and various SEVIS II reports. SEVIS II is also the source of the admissibility indicator and employment eligibility determination for F/M/J nonimmigrants.

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

Federal law requires the collection of information about F/M/J nonimmigrants and the maintenance of the SEVIS II system. The information is collected to maintain current information on



F/M/J nonimmigrants during the course of their stay in the U.S. SEVIS II facilitates DHS and DOS oversight and enforcement activities concerning F/M/J nonimmigrants, schools, and sponsors, to ensure compliance with applicable federal laws and regulations. Table 2 lists the specific information in SEVIS II and why it is needed.

Table 2: PII Collection Justification

Category of Information	Personally Identifiable Information	Purpose
Non-Governmental SEVIS II User Account Information (For F/M/J nonimmigrants and dependents and school and sponsor officials, owners, chief executives, legal counsel and/or proxies, parents, or guardians.)	Name, Address (Domestic and Foreign), and Date of Birth	Used to identify unique individuals and to communicate with F/M/J nonimmigrants as well as schools/sponsors.
	Birth Country and City Country of Citizenship Country of Legal Permanent Residence	Used to help identify F/M/J nonimmigrants Used to enforce the requirement that only U.S. citizens or lawful permanent residents can serve as school or sponsor officials.
	Username E-mail addresses	Used for account management, tracking a user's system activity, and communication with users.
	Immigrant Identification Number (IIN)	IINs are issued to all SEVIS II users, including school or sponsor officials who are U.S. citizens, and are used to uniquely identify SEVIS II users.
	Alien Registration Number (DHS-assigned number)	Used to verify that a school or sponsor official is a U.S. lawful permanent resident.
	National Identity Number (assigned by foreign governments to their citizens and residents; not a U.S. identity number)	Used to match nonimmigrant users to their own SEVIS II records, and school/sponsor users to their school/sponsor SEVIS II records. Required for South Korean nationals as there are very few last names in South Korea so the National Identity Number is needed to identify records about the same person.
	Passport – optional (number, issuing country, expiration date)	Used as secondary identifier to confirm unique individual biographic information as passport information is generally unique to an individual.
F/M/J Principal Nonimmigrant Educational and Financial Information	Program of study – educational level and major, secondary major, and minor) School Registration Information (major, course and registration information, program completion information, drop below full course information) for F and M nonimmigrants	Required to ensure F and M nonimmigrants are complying with immigration law related to the class of admission. Used to conduct trend analysis for counterintelligence and counterterrorism purposes.



Category of Information	Personally Identifiable Information	Purpose
	Program completion or termination information Transfer information Out of country information and Study Abroad Extensions Change of Educational Level	Used to confirm enrollment in SEVP-approved institution and for monitoring compliance with immigration laws.
	Student ID Number (number issued by U.S. school, optional, F/M only)	Optional information to help schools reconcile SEVIS II data with school databases.
	I-901 Fee Payment Information. Financial Information (For F and 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)	Required to determine individual’s ability to pay school costs and related expenses, which is an eligibility requirement for F and M status. DOS Consular Affairs takes into account financial information when making a visa issuance determination.
F/M/J Nonimmigrant Status and Benefit Information	Fingerprint Identification Number	For nonimmigrants over 14 years of age, used to identify records about the same individual and reduce fraud through biometric verification. Fingerprints are not collected on nonimmigrants under the age of 14.
	Visa (number, issuing country, expiration date)	Used as a primary data element in the generation of the admissibility indicators and to conduct analysis determining compliance with immigration law.
	Class of Admission	Used to identify F/M/J nonimmigrants; assists in determining that nonimmigrants are remaining in status and complying with all immigration laws applicable to the appropriate class of admission.
	Immigrant Benefit Application Adjudication Information (212(e) Waiver, etc.)	Results of adjudication decisions maintain the person-centric data management methodology, and to ensure consistency of information across immigration benefit determination systems.
	Arrival and departure information (POE and date of entry/exit)	Used to ensure that F/M/J nonimmigrants are remaining in status and complying with all immigration laws applicable to the appropriate class of admission. Arrival and departure information also helps to generate and update the admissibility indicator.
	Homeland Security Flag	Used to identify individuals that meet specified homeland security threat criteria who may require further investigation



1.4 How is the information collected?

SEVIS II collects information from F/M/J nonimmigrants and school/sponsor officials through SEVIS II and from other federal data systems (identified in Question 1.2 above) through electronic system-to-system interfaces. Various forms used by DHS, DOS and other federal agencies collect the information described in this PIA from individuals, schools, and sponsors. Table 3 lists the various forms used, including the Office of Management and Budget (OMB) Control Number for each form pursuant to the Paperwork Reduction Act.

Table 3: Information Collection Forms

Category of Information Collected	Form
F/M/J nonimmigrants	<p><u>U.S. Department of Homeland Security Form I-20</u> "Certificate of Eligibility for Nonimmigrant (F-1) Student Status for Academic and Language Students," OMB Control No. 1653-0038</p> <p><u>U.S. Department of State Form DS-2019</u>, "Certificate of Eligibility for Exchange Visitor (J-1) Status," OMB Control No. 1405-0119</p> <p><u>U.S. Department of State Form DS-7002</u>, "Training/Internship Placement Plan", OMB Control No. 1405-0170</p> <p><u>U.S. Department of Homeland Security SEVIS I-901</u> "Student and Exchange Visitor Program SEVIS I-901 Fee," OMB Control No. 1653-0034</p> <p><u>U.S. Department of Homeland Security Form I-765</u>, "Application for Employment Authorization," OMB Control No. 1615-0040</p> <p><u>U.S. Department of Homeland Security Form I-539</u>, "Application to Extend/Change Nonimmigrant Status," OMB Control No. 1615-0003</p> <p><u>U.S. Department of Homeland Security Form I-94</u>, "Arrival/Departure Record," OMB Control No. 1651-0111</p>
School	<p><u>U.S. Department of Homeland Security Form I-17</u> "Petition for Approval of School for Attendance by Nonimmigrant Student," OMB Control No. 1653-0538</p>
Sponsor	<p><u>U.S. Department of State Form DS-3036</u>, "Exchange Visitor Program Application," OMB Control No. 1405-0147</p> <p><u>U.S. Department of State Form DS-3037</u>, "Update of Information on Exchange Visitor Program Sponsor", OMB Control No. 1405-0147</p> <p><u>U.S. Department of State Form DS-3097</u>, "Annual Report, J-1 Exchange Visitor Program," OMB Control No. 1405-0151</p>



1.5 How will the information be checked for accuracy?

SEVIS II obtains the information directly from the individual through direct user input or from other federal agencies (identified in Question 1.2 above) that generate the information or collect the data from the individual. For data received from other agencies, it is the responsibility of the original data collector to ensure the accuracy of information provided to SEVIS II. Because the individual typically serves as the source of SEVIS II data, the data is considered to be very accurate.

Data about F/M/J Nonimmigrants

To ensure the information provided by F/M/J nonimmigrants who input data into SEVIS II is accurate, SEVIS II employs field-level validation that ensures that data inputs correspond with appropriate field parameters (e.g., ensuring only a date will be entered into a date field or a name into a name field). F/M/J nonimmigrants are able to access their own information through SEVIS II to see if errors exist. All F/M/J nonimmigrants over the age of 14 must certify under penalty of perjury the accuracy of information they enter into SEVIS II using an electronic signature. The electronic signature will require the SEVIS II user to input their username and PIN to authenticate their identity and ensure completion by the appropriate user.

Some data on nonimmigrants is verified through interfaces with other federal information systems to ensure that information in SEVIS II is accurate. For example, U.S. consular officials often update the spelling of nonimmigrants' names in the DOS Consular Consolidated Database if they do not match the spelling on the passport. SEVIS II will receive updates from this database to ensure that information in SEVIS II matches what is on the passport. Additionally, CBP officers at the U.S. port of entry electronically match the passport information to the existing SEVIS II record. If discrepancies exist, the CBP-collected passport information overrides the existing information in SEVIS II, thereby ensuring the most accurate information in SEVIS II.

If information in the SEVIS II system is inaccurate, an F/M/J nonimmigrant may submit a change request to the SEVIS II help desk. The help desk will evaluate the request, make any changes deemed appropriate to correct the data, and send a response approving or denying the request to the nonimmigrant and their school or sponsor.

Data Received from other Federal Data Systems

SEVIS II software monitors information received through the electronic interfaces from other DHS and DOS systems on a daily basis. SEVIS II software actively monitors interfaces and generates reports on any errors encountered during data transfers, including discrepancies in the data. If the data is not consistent with the information already in SEVIS II, SEVIS II rejects the record, an interface error log documents the data, and the error log is available to the other DHS and DOS systems.

Data Migrated to SEVIS II

SEVP is conducting rigorous validation and accuracy checks on the information migrated from the SEVIS legacy system to the SEVIS II system. During data migration, SEVP merges the legacy records to create a one-person, one-record structure for F/M/J nonimmigrants using an entity resolution process and software tools that rely on matching parameters and weights established by the SEVIS II Data



Management Working Group (DMWG). The merging process will occur in an iterative fashion, with results being reviewed by the DMWG and changes being made to the matching algorithms as needed to enhance the accuracy of the matching and merging process. To further mitigate against the risk of information corruption, SEVIS II will conduct address verification using commercial software during the migration of SEVIS data.

Upon creating an account in SEVIS II, F/M/J nonimmigrants and school/sponsor officials must validate whether or not any of the merged legacy records are in fact theirs. If they believe that certain data in a merged record or that one or more of the merged records does not pertain to them, they can request to have the erroneous records decoupled (i.e., unmerged) in their account. A request for decoupling made in the individual's account generates a ticket for the SEVIS II help desk. In addition, the system allows the F/M/J nonimmigrant to provide information that is missing. If an F/M/J nonimmigrant recognizes that a previous record that should appear in their account is missing, they can submit a SEVIS II help desk ticket. The individual indicates which record is missing and is prompted to provide, to the best of their ability, the missing information.

The merging and decoupling (i.e., correction) of records migrated from the SEVIS legacy database is necessary to complete the transition from the SEVIS record-centric to SEVIS II person-centric data management methodology. The migration of data will affect records pertaining to F/M/J nonimmigrants, schools, and sponsors.

SEVIS II requires additional data elements about the F/M/J nonimmigrant that were not captured in the legacy SEVIS database, specifically, the data elements collected as part of the customer account information.⁴ Additionally, some data elements in SEVIS will not be used in SEVIS II and therefore will not be migrated to the new system (i.e., Social Security Numbers, driver license information).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The legal authority to collect this information is 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 (DMIA); Public Law 106-396, Visa Waiver Permanent Program Act of 2000 (VWPPA); Public Law 107-56, U.S.A. PATRIOT Act; and Public Law 107-173, Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act). The collection of information is mandated by 8 CFR 214.2(f), (j), and (m), 214.3, and 214.4, and 22 CFR Part 62.

⁴ Those data elements are the IIN, national identity number, physical U.S. address, alternate names, multiple email addresses, country of lawful residence, multiple countries of citizenship, and additional employment information (employer name, EIN, and employment eligibility dates).



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

The collection of information presents inherent privacy risks, including the possible misuse and inappropriate dissemination of data. Given the extent of the information collected within the SEVIS II database, there is a risk of abuse if any individual(s) has access to the entirety of the system, or records in the system that extend beyond the individual user's need to know. To mitigate this risk, role-based permissions determine a user's access to SEVIS II records. F/M/J nonimmigrants will only be able to access information contained within their own accounts for themselves and any dependents for which they are inputting data. Proxies, parents, and guardians will be able to access only those records they have created. School and sponsor officials will have access to only those SEVIS II records pertaining to F/M/J nonimmigrants enrolled with that particular school or sponsor. For government SEVIS II users, the system only provides access to users who need the information to effectively perform assigned job functions. All authorized users must go through an approval process and only access SEVIS II through approved equipment or through an appropriate web interface reflecting necessary role and responsibility access privileges.

DHS has a legislative mandate to collect and maintain current information relating to F/M/J nonimmigrants during the course of their stay in the U.S. SEVIS II collects information that effectively and efficiently carries out the purposes of the program. Wherever possible, the individual directly provides information about him or herself, thereby greatly enhancing the accuracy of information in the system. In addition, the system uses information from other federal information systems to validate the F/M/J nonimmigrant data and will allow information deemed to have greater accuracy to overwrite SEVIS II data (e.g., passport data collected at the border). The most significant mitigation to the risk of inaccurate data is the individual's ability to view their own data in the system and request that SEVP correct inaccurate information through the submission of a help desk ticket.

The migration of historical data from the legacy SEVIS to SEVIS II represents a privacy risk as the potential exists that merging records will result in erroneous coupling of records that are not about the same individual, or other information corruption or duplication. To mitigate this risk, ICE has undertaken several procedural safeguards during the migration process to minimize the risk of data errors. At the end of the process, the individuals that are the subjects of these records will be able to access the migrated data and verify whether merged records are in fact theirs. Individuals may submit a request to the SEVIS II help desk to correct any errors that arose out of the migration.

Finally, SEVIS II is reducing the collection of sensitive PII by eliminating the collection and maintenance of both the Social Security Number and driver's license information that was previously collected by the legacy system. The removal of these two sensitive data elements enhances privacy by minimizing collection of data and reducing the risk of identity theft if the SEVIS II database is compromised.



Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The U.S. Government uses SEVIS II to execute the legislative mandate requiring the collection of information on F/M/J nonimmigrants. Specifically, ICE and DOS use information about F/M/J nonimmigrants to ensure that they comply with the obligations of their U.S. admittance and to maintain a history of their status-related activities. ICE, as well as DOS, uses the information to identify and act on potential compliance violations by both schools and sponsors. ICE uses the information in statistical form to publish a quarterly compilation of information concerning schools, sponsors, and F/M/J nonimmigrants.

In the SEVIS II system, the F/M/J nonimmigrant biographic information populates a certificate of eligibility (Form I-20 for F and M or Form DS-2019 for J) for F/M/J nonimmigrants accepted by a U.S. school or sponsor. Additional programmatic information (i.e. educational record, financial information) completes the certificate of eligibility. The completed certificate is a prerequisite for applying for a visa. U.S. consulates use the information contained within the certificate of eligibility (Form I-20 or DS-2019) as a component of the visa issuance decision-making process. U.S. consulates and schools also use F/M nonimmigrants' financial information to determine their ability to pay for the program, which is a prerequisite to obtaining an F or M visa. DOS Consular Affairs also takes into account financial information when making a visa issuance determination for F/M/J nonimmigrants.

SEVIS II uses the visa issuance information, other information already in the system, and a set of business rules to generate an admissibility indicator. CBP officials use the admissibility indicator (available to them through TECS) when the F/M/J nonimmigrant arrives at the port of entry and requests admission. The admissibility indicator is a component of the CBP officials' decision to admit the nonimmigrant the U.S.

USCIS officials use SEVIS II information to assist in determining the eligibility for a change of status or for benefits associated with their class of admission through SEVIS II interfaces with CLAIMS, Verification Information System, and E-Verify. SEVIS II will use information in the system and predefined business rules to determine employment eligibility when queried by E-Verify regarding a nonimmigrant's employment status.

FBI, FTTTF, and ICE use SEVIS II information to perform trend analysis for counterintelligence and counterterrorism purposes, and for investigations of violations of criminal and immigration laws.

Finally, SEVIS II uses biographic information (i.e., name, citizenship, date of birth, etc.) to create non-government SEVIS II accounts. SEVIS II then assigns an IIN to all non-government SEVIS II users, including school and sponsor officials. Once an individual's account is created, the IIN is used within SEVIS II to maintain the "one person-one record" data management methodology.



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

SEVIS II provides information technology (IT) tools to assist users in monitoring the status of F/M/J nonimmigrants. Specifically, SEVIS II has predefined business rules that use information in the system to create simple reports and to generate the system's admissibility indicator and employment eligibility determination.

As discussed above, the admissibility indicator reflects whether an individual is eligible for admission to the U.S. as an F/M/J nonimmigrant. This indicator is visible to F/M/J nonimmigrants through SEVIS II and to CBP officers through TECS. The admissibility indicator has three possible values:

- Eligible for admission (Green)
- Not eligible (Red)
- May be eligible (Yellow)

The SEVIS II admissibility indicator is generated using business rules applied to information in the F/M/J nonimmigrant record, resulting in the appropriate Green/Red/Yellow indicator as the value for this field. For example, an F/M/J nonimmigrant will not be eligible for admission until thirty days prior to their program start date, so the SEVIS II record will reflect a Red admissibility indicator until that time.⁵ Alternatively, SEVIS II will transmit the conditional entry indicator (Yellow) if there are outstanding issues when an F/M/J nonimmigrant arrives at the POE (e.g., a student whose previous period of status was terminated due to inability to pay tuition may be asked to prove financial ability before he will be admitted). A Yellow indicator requires that the CBP officer should review additional information in SEVIS II through the SIGMA interface (described in Question 4.0) to adjudicate the admission request.

The SEVIS II employment eligibility determination reflects whether an F/M/J nonimmigrant is legally eligible for employment during their stay, the length of eligibility, and whether a nonimmigrant can work for one or multiple employers. SEVIS II will transmit this information to the E-Verify system upon request. Like the admissibility indicator, the employment eligibility determinations will also be visible to F/M/J nonimmigrants through SEVIS II.

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

SEVIS II uses commercial data software to provide address verification. The software validates input address information during the migration of historical data from the SEVIS database to SEVIS II. SEVIS II also employs the software in the production environment, verifying the U.S. addresses of applicants. The software does not create any connections outside of SEVIS II nor does it transmit any information. When an applicant inputs an address that the software cannot validate (i.e., new construction), the system

⁵ F and M nonimmigrants in a short term program will not be eligible for admission until fifteen days prior to their program start date.



will allow the input, and flag the address for further inspection, either at a later date when the address database is refreshed or by an ICE analyst.

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

Access to the information is restricted to authorized users from schools, sponsors, DHS, DOS, and other government agencies. In addition, F/M/J nonimmigrants have limited access to individual account information. Physical and computer safeguards are in place to prevent unauthorized persons from gaining access to the data. To prevent inappropriate access by unauthorized personnel or misuse of data, computer safeguards exist throughout the system, including password protection, firewalls, and extensive audit trails. SEVIS II records and maintains information on session activity (e.g., user ID, log on time, duration of session, and log off time) each time a user accesses the system.

SEVIS II generates decisions regarding admissibility and employment eligibility based upon system information and preexisting business rules. To mitigate the risk that SEVIS II incorrectly indicates a lack of employment eligibility, if the F/M/J nonimmigrant believes that a decision was made in error, they may file an appeal through SEVIS II per the SEVIS SORN and the system's determination will be reviewed by SEVP personnel. If the F/M/J nonimmigrant believes the admissibility indicator displayed on SEVIS II is inaccurate, the individual may submit a help desk ticket requesting that the indicator value be reviewed. Government personnel review such requests and update SEVIS II records to correct errors. SEVP personnel periodically review correction information and proactively addresses business rule errors responsible for causing multiple incorrect benefit adjudication decisions.

During the initial months of SEVIS II operation, a SEVP task force will further mitigate the risk that CBP officers at ports of entry may incorrectly deny access to an F/M/J nonimmigrant because of an erroneous SEVIS II admissibility indicator. If a problem arises upon entry, CBP officers will be able to contact the task force for guidance and clarification of the admissibility decision. In addition, a CBP officer in secondary inspection at the port of entry will review any denial of admission initiated by a CBP officer because of the SEVIS II indicator. The review by a secondary officer mitigates the risk that a system-generated denial is an error, and provides a human validation of the denial determination.

In addition, SEVIS II maintains a record of all changes that a user makes to the data in the system. These features provide an audit trail of all user actions. The audit trail allows for the monitoring and analysis of user activity to identify inappropriate use of the system.

Section 3.0 Retention

3.1 What information is retained?

The SEVIS II retains system inputs (including ingests from other systems, online entries made by F/M/J nonimmigrants and school and sponsor officials); the master file; outputs (reports); government and non-government user account information; and user audit information.



The data from legacy SEVIS will be migrated to SEVIS II but also retained separately.

3.2 How long is information retained?

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 from the date of last transaction.

A copy of the data from the original SEVIS system, which will be maintained separately retained from SEVIS II, will be retained for seven (7) years.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration?

No. ICE has drafted a proposed retention schedule for SEVIS II. A retention schedule exists for the original SEVIS system but it does not adequately describe all data maintained in SEVIS II.

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

The 75-year retention period for the master file in SEVIS II is consistent with the policy of the U.S. Government to retain records related to immigration for the approximate lifetime of an individual. This information is necessary for the time indicated for historical purposes and because specific immigration-related law enforcement or benefit activities can span decades. Security measures taken mitigate the risk associated with the length of retention in accordance to DHS security policies, requiring explicit roles and responsibilities limiting access to information exclusively to those individuals who require access to complete essential job functions.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

SEVIS II shares F/M/J nonimmigrant status information with US-VISIT's ADIS. The information shared with ADIS on F/M/J nonimmigrants determines which individuals are no longer in active status and must exit the U.S. This information sharing is necessary for monitoring compliance with immigration law.



SEVIS II exports F/M/J nonimmigrant information to USCIS's Verification Information System (VIS) for determining immigration benefits entitlement. USCIS users can query SEVIS II data through the USCIS Enterprise Service Bus (ESB) to help government agencies verify the immigration status of an individual that has applied for a government benefit to ensure eligibility for federal, state, or local public benefits and licenses.

SEVIS II sends employment eligibility information to USCIS's E-Verify when queried by the system. USCIS uses the employment eligibility information in the adjudication of employment benefit decisions.

SEVIS II shares information with CBP's TECS. Through TECS, CBP officers can view the latest F/M/J admissibility indicator from SEVIS II for individuals who are at or about to arrive at the port of entry.

Finally, SEVIS II shares information with CBP's Secured Integrated Government Mainframe Access (SIGMA) system. SIGMA users query SEVIS II data to retrieve additional information that is not in TECS about an F/M/J nonimmigrant who has requested admission at the port of entry. CBP uses this information to help determine whether to admit the nonimmigrant to the U.S.

4.2 How is the information transmitted or disclosed?

Information shared with VIS, E-Verify, TECS, and SIGMA transmits through the USCIS ESB interface. Instead of accessing multiple federal information systems, the interface allows DHS users to make a single query request. The interface accesses the individual systems including SEVIS II and presents the responsive data as a consolidated set. The secure socket layer (SSL) protocol secures the transmission of data. A separate PIA for the ESB is available on the Privacy Office website, www.dhs.gov/privacy.

SEVIS II and US-VISIT/ADIS transmit information through a secure electronic web-based interface. Information exchanges occur daily between ADIS and SEVIS II using US-VISIT's proprietary eXtensible markup language (XML).

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

Sharing of SEVIS II information within DHS is for carrying out activities related to the F/M/J nonimmigrants travel to and from the U.S., and their requests for any immigration related benefits, such as employment benefits. The sharing of this information with CBP supports the narrow purpose of admitting the F/M/J nonimmigrants to the U.S. in accordance with the terms of their class of admission. The sharing of information with USCIS is to support the appropriate determination of requests for employment and other immigration benefits, or to support USCIS programs designed to ensure that only nonimmigrants who are actually eligible for government benefits receive them. The sharing of this information is therefore consistent with the purposes for which it was collected, namely to ensure the



appropriate administration and enforcement of the student and exchange visitor laws and regulations, and to track F/M/J nonimmigrants here in the U.S. and ensure they comply with the terms of their admission.

The privacy risks associated with each step of internal sharing, including system and network security, data, usage, data transmission, and disclosure have been identified and mitigated through adherence to DHS policies and procedures, such as System Design Lifecycle documentation and Certification and Accreditation (C&A) documentation. Internal sharing of data is conducted over secured networks controlled by DHS, utilizing DHS approved computers, services, and software. In addition, only authorized users who need the information contained in SEVIS II have access to the system and all authorized users are assigned appropriate roles and responsibility access appropriate to their functional need.

There will always be the possibility of misuse and inappropriate dissemination of information despite the above described technical security aspects. Security logs, audit logs of user activity, and strict access controls help mitigate these risks. A user's supervisor must approve system access. The DHS/Office of the Chief Information Officer utilizes an Active Directory to authenticate a user to SEVIS II. SEVP administers role-based access to ensure that only those users with a management-approved functional need and appropriate security clearance receive approval for SEVIS II use.

SEVIS II records and maintains information on session activity (e.g., user ID, log on time, duration of session, and log off time) each time a user accesses the system. In addition, SEVIS II maintains a record of all changes that a user makes to the data in the system. These features provide an audit trail of all user actions that monitor and analyze user activity for compliance. These features also provide a means to ensure data integrity.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Personnel at two federal agencies outside DHS are granted direct user access to SEVIS II: DOS and the FBI. DOS Office of Private Sector Exchange (OPSE) users directly access SEVIS II to administer the Exchange Visitor Program, e.g., the processing of applications for designation of Exchange Visitor Program sponsors. DOS Consular Affairs users access SEVIS II to verify the validity of information when issuing visas to nonimmigrants and checking immigration benefit eligibility. DOS OPSE and Consulate Affairs users may access all information contained within SEVIS II. FBI users directly access SEVIS II to perform counterintelligence and counterterrorism analysis.

In addition, SEVIS II regularly exports data to the FBI's FTTTF, which analyzes SEVIS II data to support the FBI's counterterrorism mission.

SEVIS II also sends the IIN for F/M/J nonimmigrants to the Treasury Department's I-901 fee payment interface to verify payment of the SEVP fee due to ICE from the F/M/J nonimmigrant. This information sharing allows SEVIS II to ensure that payment information submitted through the I-901 system matches F/M/J data currently in SEVIS II.



In addition, school and sponsor officials directly access SEVIS II to create user-generated reports and extract data. The reports may contain F/M/J nonimmigrant biographic and status information, but the school and sponsor access is limited to only those F/M/J nonimmigrants enrolled by that particular school or sponsor. Schools and sponsors use this information to manage their responsibilities under federal law with respect to the F/M/J nonimmigrants enrolled in their schools or Exchange Visitor Programs.

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

The sharing of information with DOS, Treasury, and the schools and sponsors is compatible with the purposes of the original collection, namely to ensure the appropriate administration and enforcement of the student and exchange visitor laws and regulations, and to track F/M/J nonimmigrants here in the U.S. and ensure they comply with the terms of their admission. Sharing of SEVIS II information with the FBI is necessary to support counterterrorism and counterintelligence programs critical to national security. All sharing of information from SEVIS II is pursuant to an applicable routine use in the SEVIS SORN. Memoranda of Understanding exist between SEVIS II and DOS, U.S. Treasury (I-901), and the FBI. These agreements appropriately define the information sharing and usage of information.

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

SEVIS II shares information with FBI and DOS OPSE personnel, which have direct access as users of SEVIS II. Security logs, audit logs, and strict access controls safeguard SEVIS II information sharing occurring through government user accounts.

SEVIS II shares information electronically with DOS Consulate Affairs through the USCIS ESB web service. Transmission of data sent through the USCIS ESB secures through the SSL protocol using public key infrastructure (PKI) authentication measures.

Information is shared in bulk with the FBI FTTTF via an electronic export using a secure XML web connection. Information shared with the U.S. Treasury's I-901 web service interface takes place through SSL and PKI authentication.

SEVIS II applies all sensitive data (e.g., PII data, passwords) identified and appropriate encryption technologies to ensure the confidentiality and integrity of sensitive data. All SEVIS II cryptographic operations perform using FIPS 180-2-approved algorithms.



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

Allowing external users access to a system raises the risk of inappropriate use and access. In the case of SEVIS II, this risk is mitigated by the fact that SEVIS II records and maintains session activity (e.g., user ID, log on time, duration of session, and log off time) each time a user accesses the system. In addition, SEVIS II maintains a record of all changes that a user makes to the data in the system. These features provide an audit trail of all user actions that monitors and analyzes user activity for compliance. SEVP reviews the audit trails through weekly security audit reports to ensure appropriate access to and use of data. These features also provide a means to ensure data integrity.

Because SEVIS II is accessible by non-government users (i.e., schools, sponsors, and F/M/J nonimmigrants), there is an additional privacy risk of access by unauthorized persons and inappropriate use associated with this system. The measures and processes put in place for school certification, sponsor designation, and ID/password issuance offsets and minimizes this privacy risk. In addition, the design of SEVIS II separates critical system components from the public. The public will only interface with the web-enabled front end of the system delivered via the DHS Portal. Business processes, logic functions, and database access will not be publicly accessible.

In addition, the risks of external sharing of data are mitigated because SEVIS II sharing occurs over secured networks. Only authorized users will handle biographic and biometric data. Sharing data with DOS personnel will take place through the secured and encrypted web-based user interface. There is a possibility of misuse and inappropriate dissemination despite the technical security considerations; however, taking advantage of DHS security policies that require audit logs of user activities, security logs, and strict access controls mitigates these risks.

Section 6.0 Notice

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

This PIA provides general notice about the collection of this information, the amended SEVIS SORN, and the publication of a Notice of Public Rulemaking. Non-government SEVIS II users will be notified by a Privacy Act Notice when completing the Form I-17, the Form I-20 and/or the Form DS-3036, Form DS-3037, Form DS-3097, Form DS-2019 and Form DS-7002. All non-government SEVIS II users will also receive notice through a Privacy Act Notice on SEVIS II that will display before asking to provide any personal information.



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

Yes, however the failure to provide requested information would preclude the non-government SEVIS II users from accessing the functionality of SEVIS II and prevent the individual from receiving the benefits sought.

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

No, system users consent to all uses of their information through electing to create an account and the submission of information to SEVIS II. SEVIS II presents a Privacy Act Notice detailing authority and uses of information to all non-government users. The form also contains a signature certification and authorization to release any information from an applicant record that SEVIS II needs to determine eligibility, which includes biographic and biometric data.

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

There is a risk that individuals may be unaware of the nature of information collected about them for the SEVP, and how it will be used and shared. This risk is mitigated by the notice provided to individuals whose information is collected by and maintained in the SEVIS II system at the time of collection. In addition, this PIA and the SEVIS SORN provide additional public notice of the nature, purpose, use, and sharing of the information about individuals. F/M/J nonimmigrants may also view the information collected about them and verify portions of their information in SEVIS II.

Section 7.0 Access, Redress and Correction

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

F/M/J nonimmigrants can view information about themselves in the system by logging into SEVIS II. School and sponsor SEVIS II users can view their own information provided for account setup purposes through the system as well.

In addition, individuals may request access to records about them in SEVIS II by following the procedures outlined in the SEVIS SORN. Some of the requested information may be exempt from access pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests. Providing individual access to records contained in SEVIS II could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or



another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Adverse determinations under the USCIS E-Verify program may be appealed pursuant to the E-Verify appeal procedures, which are included in notices of adverse determinations provided to individuals and described in the USCIS Verification Information System Privacy Impact Assessment dated April 2, 2007. In instances where SEVIS II data is the basis for an adverse determination for employment authorization, the individual may review their SEVIS II record and seek to correct information they believe to be in error in accordance with the procedures described below in Question 7.2.

In addition to the procedures above, 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:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia/index.htm>). 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, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

To correct inaccurate or outdated information in the system, an F/M/J nonimmigrant will have the opportunity to edit specific data fields including address and employment. If an error exists in information fields they or their school or sponsor official are not able to correct, or if the F/M/J nonimmigrant believes the admissibility indicator displayed in the system is inaccurate, they will be able to submit a SEVIS II help desk ticket to update the information. A government user at SEVP or DOS OPSE will review the request, inspect the submitted information, and contact the nonimmigrant via email if additional information or justifying documentation is required. The government user will then either deny the request or accept and complete the account information modification. The government user will communicate the final determination to the nonimmigrant user, and the nonimmigrant requestor may view the determination by accessing the SEVIS II account.

During the initial months of SEVIS II's operation, a SEVP task force will exist to mitigate the risk that CBP officers at ports of entry may incorrectly deny access to an F/M/J nonimmigrant because of an erroneous SEVIS II admissibility indicator. If a problem arises upon entry, CBP officers will be able to contact the task force for guidance and clarification of the admissibility decision. In addition, a CBP officer in secondary inspection at the port of entry will review any denial of admission initiated by a CBP officer because of the SEVIS II indicator. The review by a secondary officer mitigates the risk that a system-generated denial is an error, and provides a human validation of the denial determination.



If individuals obtain access to the information in SEVIS II pursuant to the procedures outlined in the SEVIS SORN and not through the web interface, they may seek correction of any incorrect information in the system by submitting a written request to correct the data. The SEVIS SORN outlines the data correction procedures. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, 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:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (<http://www.ice.gov/foia/index.htm>). 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, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

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

The SEVIS II website notifies individuals of the procedures for correction, as do the published PIA and SORN.

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

Formal redress is provided, as described above, for information maintained in the SEVIS II system. In addition, because SEVIS II generates decisions regarding employment eligibility, F/M/J nonimmigrants who believe that an employment eligibility decision was made in error may file an appeal through E-Verify and if necessary seek to correct their SEVIS II records in accordance with the procedures described above.

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

The Privacy Act provides access and other procedural rights, with the exceptions noted above. The risks associated with redress include misuse or abuse of the redress program, misuse or loss of data, inadvertent release of data, and identity theft. The direct involvement of a government user in the



evaluation and decision making process for each individual case mitigates the associated risks. The existence of the robust SEVIS II auditing system further mitigates the risk of abuse. Beyond direct user evaluation, the use of the auditing function will allow for monitoring and reporting on anomalous user activity.

Section 8.0 Technical Access and Security

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

DHS has documented standard operating procedures to determine which users may access SEVIS II. Access for SEVIS II internal and external users vary depending on their established role-based privileges. SEVIS II will have three classes of users, with separate access protocols. The three classes are as follows:

- **DHS Users:** DHS users receive access to SEVIS II based upon role and relevant job need. Users receive one of four permission levels: read only access, read and report access, limited editing capability (primarily help desk support), and complete read/write access (super user). Permissions also establish whether the user may access information pertaining to all SEVIS II users, or to a limited subset.
- **Other Government Users (FBI, DOS Users):** DOS users within OPSE receive permissions similar to those assigned to DHS. Users may receive one of four permission levels; read only access, read and report access, limited editing capability, and complete read/write access (super user). FBI users all receive read-only access to SEVIS II.
- **Non-government SEVIS II Users (For F/M/J nonimmigrants, school and sponsor officials, owners, chief executives, legal counsel, and/or proxies, parents, or guardians):** F/M/J users may only access information contained within their individual accounts, and have the ability to update only certain fields in the system. School and sponsor officials may only access information for those nonimmigrants enrolled or participating within their specific program(s). School and sponsor officials may update certain information within the system for F/M/J nonimmigrants enrolled or participating in their specific program(s), as well as update information on the school and exchange visitor program sponsor. Proxies, parents, and guardians may view only their own account and those they have created for an F/M/J nonimmigrant.

8.2 Will Department contractors have access to the system?

Yes. Contractors who possess a favorably adjudicated clearance will have access as necessary to maintain SEVIS II and provide technical support. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate nondisclosure and use limitations. ICE personnel will determine access levels.



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

As detailed in Questions 8.1 and 8.2, all SEVIS II users will have limited role-based access. SEVIS II users will receive role-based system-specific training intended to ensure compliance with use limitations and other safeguards discussed in this PIA. Specifically, all SEVIS II government and non-government users will complete web-based, self-paced training designed to familiarize account holders with the system. SEVP requires all school officials to complete training. OPSE also requires training for all sponsors officials. Both SEVP and OPSE conduct training for school and sponsor officials at conferences. SEVIS II will also provide specific training for users with a job requirement to create data extracts or print reports. In addition, all internal DHS, DOS, and DOJ users will have to accept and sign the system's Rules of Behavior document.

In addition, all ICE personnel and contractors complete annual mandatory privacy and security training and training on "Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information."

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

The C&A process is in progress but is expected to be complete in early 2010.

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

SEVIS II audits all user activity to prevent misuse of SEVIS II data. For each user session, SEVIS II logs the user ID, log on time, duration of session, and the log off time. The SEVIS II audit log additionally tracks data entry, modification, and/or deletion of existing data by the individual responsible for the action. SEVP reviews the audit trails through a weekly security audit report to ensure appropriate access to and use of SEVIS II data. If a SEVP user's account activity appears inconsistent with task requirements, SEVP will follow up with the user to determine the root cause of the anomaly. In circumstances where SEVP determines that unauthorized access to or misuse of data has occurred, SEVP terminates any user account responsible for the activity.

Ensuring that all SEVIS II data is stored in compliance with the requirements of the DHS IT security policy (e.g., DHS 4300A Sensitive System Handbook) further mitigates the risk of data misuse. In accordance with the program dictated by the DHS 4300A Sensitive System Handbook, management, operational, and technical controls instituted ensure that all information contained within SEVIS II is protected according to best practice standards. The system's C&A, based on NIST 800-53 "Recommended Security Controls for Federal Information Systems," will fully examine the system for security vulnerabilities. Identified critical vulnerabilities will be addressed before the system is deployed; a Plan of Action and Milestones will track acceptable risks.



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

The security risks include unauthorized system access or use, inadequate system security, the extensive external and internal data sharing required to perform the functions legislatively prescribed to the SEVIS II database; however, the issuance of guidance restricting data access and establishing strict user authentication and role-based access have substantially mitigated these risks. The required system specific privacy and security training that all users must complete and recertify on an annual basis further mitigate these risks. Extensive audit trails and data use monitoring are in place to prevent the abuse of system access and data use.

Section 9.0 Technology

9.1 What type of project is the program or system?

SEVIS II is an enterprise-wide, operational IT system supporting DHS ICE.

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

SEVIS II is in the Development stage of the ICE Enterprise Architecture Lifecycle Management System. SEVIS II development is using an iterative design methodology. The system development will be broken into 12 unique products. The finalized products will build upon each other. This PIA will be updated if any significant changes are made to the design as identified when SEVIS II is deployed.

9.3 Does the project employ technology that may raise privacy concerns? If so, please discuss their implementation.

SEVIS II uses business rules and data that exists in the system to generate data that will be relied upon to assist in determining whether to admit an F/M/J nonimmigrant to the U.S. at a port of entry, or whether an F/M/J nonimmigrant is eligible for an employment benefit (eligible to work while in the U.S.). The privacy risk presented by this SEVIS II capability is that if the rules are improperly developed, or the information in the system is inaccurate, F/M/J nonimmigrants may be improperly denied a benefit or denied admission to the U.S. ICE has implemented appropriate controls to mitigate these risks (fully described in 2.0), specifically, the careful review and testing of the business rules prior to deployment of the system, redress procedures for individuals who believe they have been adversely affected, and the ability for individuals to see and correct their own data in the system on which these system-generated decisions are based.



Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security