Privacy Impact Assessment
for the

# Student and Exchange Visitor Program (SEVP)

**DHS/ICE/PIA-001**

**February 20, 2020**


**Contact Point**
**Derek Benner**
**Executive Associate Director, Homeland Security Investigations**
**U.S. Immigration and Customs Enforcement**
**(202) 732-5100**

**Reviewing Official**
**Jonathan R. Cantor**
**Acting Chief Privacy Officer**
**Department of Homeland Security**
**(202) 343-1717**

# Abstract

The Student and Exchange Visitor Program (SEVP) was established as part of the Homeland Security Investigations (HSI) National Security Investigations Division (NSID) within U.S. Immigration and Customs Enforcement (ICE). SEVP oversees the certification of academic and vocational schools to allow enrollment of foreign nationals seeking entry into the United States as nonimmigrant students under F and M classes of admission. In addition, SEVP tracks and manages real-time information on F/M/J nonimmigrant students, their dependents, and the schools and sponsors that host these nonimmigrants, to ensure compliance with immigration laws and regulations. To facilitate the program's work, SEVP collects, uses, shares, and maintains personally identifiable information (PII) on nonimmigrant students, their dependents, and the school officials who work with SEVP for the school certification process. Finally, SEVP works with the other Components within the Department of Homeland Security (DHS) and other federal agencies to ensure compliance with all civil and criminal immigrations laws that align with HSI's national security and public safety missions.

The original Privacy Impact Assessment (PIA) for the Student Exchange Visitor Information System (SEVIS) was published on February 5, 2005, and was last updated on June 15, 2017. ICE is publishing this PIA to replace the previous SEVIS PIA and subsequent updates, and document the privacy protections that are in place for the PII collected, used, shared, and maintained by SEVP and the systems that support its mission under ICE and DHS.

# Overview

SEVP operates under the authority of 8 United States Code (U.S.C.) § 1372 in coordination with the U.S. Department of State (DOS), which oversees the operation of the Exchange Visitor (EV) Program.[1] Section 1372 requires DHS to develop and conduct a program to electronically collect, from approved educational institutions and designated EV programs in the United States, certain information about foreign nationals who have either applied or are applying for F, M, or J nonimmigrant status.[2] Section 1372 also requires that particular information be collected, such as

[1] Title 8 United States Code (U.S.C.) § 1372, Congress mandated that DHS, in consultation with the U.S. DOS and Department of Education, develop a national system to collect and maintain pertinent information on nonimmigrant students and exchange visitors, and the school and exchange visitor sponsors that host these individuals in the United States.

[2] When nonimmigrants apply for admission to the United States, they must declare their primary purpose for visiting. Based upon that purpose, U.S. immigration law recognizes several classes of admission, such as those for tourists and business travelers. For foreign nationals and exchange visitors, the U.S. immigration law recognizes the following three classes of admission: nonimmigrant students (F-1 and M-1 classes of admission), exchange visitors (J-1 class of admission), and their dependents and spouses (F-2, M-2, and J-2 classes of admission).

identifying information about the individual; field of study, status, and compliance information from educational institutions and EV programs; and the individual's date and port of entry.

In support of the ICE mission, SEVP uses established processes and information technology (IT) systems to collect, maintain, and analyze information to ensure that only legitimate nonimmigrant students or exchange visitors enter the United States and that institutions accepting nonimmigrant students or exchange visitors are certified and comply with all federal laws and regulations. In addition, SEVP coordinates with DOS regarding exchange visitors and supports law enforcement investigations that align with HSI's national security and public safety missions.

SEVP supports the application and admission of foreign nationals and their dependents seeking entry into the United States as nonimmigrant students under F and M classes of admission (hereinafter, "F and M nonimmigrants"). SEVP systems allow SEVP to oversee the tracking and management of F/M/J nonimmigrant students and their dependents to ensure compliance with immigration laws and regulations, and to ensure that their status is maintained.[3] In addition, SEVP systems maintain PII to facilitate the certification and oversight of academic and vocational schools (U.S.-based schools) that seek to enroll F and M nonimmigrant students based on federal regulation. SEVP provides guidance and training to school officials about the requirements to which both schools and their nonimmigrant students must adhere to maintain their status. Schools are recertified every two years to ensure they remain eligible for certification and have complied with all record-keeping, retention, reporting, and other requirements in accordance with regulations. Failure to comply will result in the withdrawal of the school's certification, prohibiting the school from enrolling F and M nonimmigrant students.

SEVP coordinates with DOS, which oversees the operation of the EV Program, including J nonimmigrants and their dependents, designation and re-designation of EV Program sponsors, and supports the application and admission of foreign nationals who seek entry into the United States as exchange visitors (e.g., research scholar, government visitor, au pair).[4] SEVP's activities related to the EV Program and J nonimmigrants are primarily limited to receipt, capture, and maintenance of EV Program data by SEVP-owned IT systems on behalf of DOS.

SEVP shares information with other program offices in ICE, DHS components, and other Federal Government agencies to facilitate ICE's investigative mission. ICE is responsible for

[3] Maintaining status means the F and M nonimmigrant is fulfilling the purpose for which DOS issued a visa and following the regulations associated with that purpose. For example, F and M nonimmigrant students must maintain their student status after they are granted entrance into the United States.

[4] DOS oversees exchange visitors (i.e., nonimmigrants who enter the United States on the J class of admission), and the exchange visitor programs (i.e., au pair, camp counselor, professor, physician, summer work travel). These individuals are given an opportunity to travel and gain experience in the United States. The exchange visitor programs sponsor J nonimmigrants, enabling them to come to the United States to teach, study, conduct research, demonstrate special skills, or receive on-the-job training for periods ranging from a few weeks to several years.

identifying, investigating, and taking enforcement action against foreign nationals who overstay their period of admission or otherwise violate the terms of their visa, immigrant, or nonimmigrant status. In addition, ICE is responsible for ensuring that certain organizations (e.g., schools, entities that sponsor EV programs) that facilitate the entry of nonimmigrant students and exchange visitors comply with applicable federal laws and regulations. For example, SEVP coordinates with the ICE Counterterrorism and Criminal Exploitation Unit (CTCEU) to conduct vetting on schools, school officials, and nonimmigrants for suitability when a viable investigative lead is identified by CTCEU.[5] Finally, SEVP coordinates administrative actions against schools, including the withdrawal of SEVP certification, and against students, in conjunction with and in support of criminal enforcement actions taken by law enforcement personnel.

ICE is conducting this PIA to provide information on SEVP activities; identify broad categories of information and applicable transactions; identify approved information collections; discuss information sharing partners; and identify SEVP systems that maintain PII. The appendices to this PIA provide more information about the information collected and shared by SEVP and describe the categories of data maintained, purpose and use, access, individuals affected, sources of information, and records retention for each SEVP system. The appendices will be updated when changes to SEVP's collection, use, sharing, and maintenance of PII occur.

***Categories of Individuals and Organizations***

SEVP collects, receives, captures, and maintains information on the following individuals and organizations:

- ***F and M nonimmigrants*** are foreign nationals participating in an academic or vocational program at SEVP-certified schools, as well as F and M dependents (e.g., spouse and/or minor children);
- ***J nonimmigrants*** are foreign nationals participating in DOS-designated exchange visitor programs, as well as J dependents (e.g., spouse and/or minor children);
- ***Proxy, parent, or legal guardian*** is an individual who has legal authority to make decisions or sign documents on behalf of another individual participating in an F, M, or J program (e.g., a minor, an individual with disabilities);

[5] For example, using open source via the internet to verify a school's petition as part of: certification; recertification; or unannounced review because of tips received from federal agents or the Field Representative Units (FRU) within the field. SEVIS also shares information with CTCEU's LeadTrac system on F and M students who are suspected of overstaying for further investigation. The function of LeadTrac is to vet and manage leads pertaining to visitors in the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations. See DHS/ICE/PIA-044 LeadTrac System, *available at* https://www.dhs.gov/privacy.

- ***Host families*** are U.S. citizens or lawful permanent residents who provide living arrangements for J nonimmigrants;
- ***Exchange visitor program sponsors*** are DOS-designated entities that sponsor and manage nonimmigrant exchange visitor categories, such as au pairs, research scholars, faculty, specialists, interns, government visitors, camp counselors, or summer work/traveling students, and must be designated by DOS to run an exchange visitor program and host J nonimmigrants. This includes individuals who have legal signature authority for the exchange visitor program sponsor (e.g., owner, chief executive officer [CEO], legal counsel);
- ***Schools*** are academic and vocational institutions that must be SEVP-certified to enroll F and M students;
- ***School officials*** are U.S. citizens or lawful permanent residents who submit information for school SEVP certification and recertification, and oversee F and M students enrolled at their school;
- ***School employees, partners, and representatives*** include the head of school (e.g., owner, president, CEO) or legal counsel who has legal signature authority for the school, school employees (e.g., faculty members, student recruiters) who are employed by a U.S.-based school and interact with F and M students, and school partners (e.g., contractor who builds housing facility, sports program that uses school space) who provide a service for a school or manage activities on school sites that impact F and M students but who are not employees of the school;
- ***Program officials*** are U.S. citizens or lawful permanent residents who submit information for DOS exchange visitor program sponsor designations and re-designations, and who oversee J nonimmigrants participating in programs offered by the sponsor;
- ***Financial support provider*** is an individual, organization, or government entity that provides support to F, M, or J nonimmigrants;
- ***Employers*** (e.g., supervisor, official with signature authority) of F, M, and J nonimmigrants with authority to work in the United States;
- ***Federal Government personnel*** are federal employees and contractors (hereinafter, "Federal Government personnel") who manage the SEVP program and who use information maintained by SEVP to support the DHS and ICE mission, as well as coordinate with DOS concerning the J exchange visitor program-related data. Additionally, Federal Government personnel use SEVP information to support other federal agency missions that align with DHS's and DOS's oversight of nonimmigrant

students and exchange visitors, including the Department of Education, Department of Commerce, Department of Justice – Federal Bureau of Investigation, and federal intelligence agencies;

- ***State government personnel*** are state employees and contractors who interact with Federal Government personnel and exchange information on activities related to administrative reviews and investigations;
- ***Governing bodies*** (e.g., licensing and accrediting bodies) ensure education provided by schools meets acceptable levels of quality, and grant licenses and accreditation to schools that meet these criteria; and
- ***Members of the public*** are individuals (e.g., property owners, holding companies, school officials, F, M, and J nonimmigrants, individuals of the general population) who (1) provide SEVP and DOS with information about things such as a school, program, or individual aligned with the student or EV Program (e.g., sponsors) and potential infractions or illegal activities; (2) provide SEVP with complaints or praise on performance of SEVP employees, its programs, or its regulations; or (3) reach out to SEVP for other reasons.

***Categories of Information***

SEVP collects, uses, shares and maintains various categories of information, including PII and sensitive PII,[6] about the individuals identified above.[7] The categories are as follows:

- ***Biographical*** – Specific to the F/M/J nonimmigrant; the proxy, parent, or legal guardian of an F/M/J nonimmigrant; the school official and head of the school; and the program official and CEO of the program sponsor. This includes full name; gender; date of birth; country of birth; country of citizenship; country of legal permanent residence; contact information (e.g., telephone number, email address, physical/mailing address); and full name and contact information of proxy, parent, or legal guardian for F/M/J nonimmigrant.
- ***Identity Verification*** – Specific to the F/M/J nonimmigrants, and school and program officials. Verifies that the biographical information provided matches against an

[6] "Sensitive PII" is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PIA, PII and Sensitive PII are treated the same.

[7] In coordination with DOS, SEVP receives, captures, and maintains information related to the Exchange Visitor Program on behalf of DOS. DOS, exchange visitor program sponsors and program officials, and J nonimmigrants (with limited capability) have access to the information and can access, view, add, edit, modify, and share information maintained by SEVP in the Student and Exchange Visitor Information System (SEVIS), as is appropriate. Please see Appendix B for additional information about SEVIS.

individual's identity. This includes identity documents[8] (e.g., driver's license, passport); Internet Protocol (IP) address; unique identifiers (e.g., SEVIS ID, immigration identification number [IIN], Tax Identification Number [TIN], official personal identification number [OPID], alien number [A-number], passport number, limited instances of Social Security number [SSN][9]); and biometric identifiers (i.e., fingerprint identification number [FIN]).

- ***Education***[10] – Specific to F/M/J nonimmigrants. This includes education transcripts; certificates of graduation; program of study (e.g., types of program, courses, level of education); length of study; school registration information; school admission number; school transfer information; extensions; and changes to study or activity.
- ***Exchange Visitor Program*** – Specific to J nonimmigrants and host families. Includes exchange visitor program information (e.g., type of program, program activities); placement information (e.g., site of activity, host family, host family contact information, exchange visitor program sponsor name); extensions; and changes to program or activity.
- ***Employment*** – Specific to F/M/J nonimmigrants. The information collected depends on the kind of employment authorized and may include the following: practical training information (e.g., training plan); employer and supervisor information (e.g., name of employer, name of supervisor); employer and supervisor contact information (e.g., telephone number, email address, website URL); Employer Identification Number (EIN); and employment information (e.g., position title, description of duties, Employment Authorization Document [EAD] Number).
- ***Criminal History*** – Mostly specific to school officials, but may also include schools and nonimmigrants. This includes arrest and bail information, case number, date charges were filed, case type, initial criminal offense type, date of crime, disposition and judgment date, and county jurisdiction. In the future, school and program officials with access to SEVP systems (e.g., SEVIS) may be required to undergo additional

[8] Identity documents may contain Sensitive PII that is not explicitly requested by SEVP. Identity documents are handled and maintained following DHS privacy and security policies.
[9] SEVP does not deliberately collect SSN. The majority of nonimmigrant student and exchange visitors do not have SSNs, and the collection of SSNs is not required for the system collection. However, SSNs may be collected incidentally as evidence submitted in the process of school certification may include copies of other documents containing SSNs.
[10] With respect to F/M/J nonimmigrant students and exchange visitors, education privacy provisions of the Family Educational Rights and Privacy Act (FERPA) are waived so that the student and exchange visitor program may be properly implemented. An educational agency or institution may not, by using FERPA or any regulation implementing FERPA as a basis, refuse to report information concerning an F or M nonimmigrant student or a J nonimmigrant exchange visitor that the educational agency or institution is required to report. *See 8 CFR §214.1 (h) Education privacy and F, J, and M nonimmigrants.*

vetting, including suitability and security clearance investigations that contain information related to background checks, investigations, and access determinations.

- ***Financial*** – Specific to F/M/J nonimmigrants. This includes financial support information (e.g., sources of funding and amounts); payment receipt information related to school certification and exchange visitor program sponsor designation fees; and payment receipt information for the I-901 fee.
- ***Travel*** – Specific to F/M/J nonimmigrants. This includes visa information (e.g., visa number, issuance post, issuance date, expiration date); passport information (e.g., passport number, expiration date, country issued); and arrival and departure information.
- ***Immigration-Related*** – Specific to F/M/J nonimmigrants. This includes information related to entry and exit into the United States (e.g., I-94 admission number, dates of entry and exit, ports of entry); class of admission (e.g., visa type); immigration status; adjudication decisions; and immigration benefit application information (e.g., adjustment of status).
- ***School*** – Specific to schools. This includes school name; contact information (e.g., telephone number, email address, physical/mailing address); publicly available information on open-source media sites (e.g., newspaper articles, school websites, personal and organizational social media websites and blogs, government websites, online forums); school's program information (e.g., site locations, addresses, phone numbers, school codes); school's accreditation and certification information and documentation; and documented evidence from nonaccredited schools (e.g., articulation agreements, state-issued professional licenses).
- ***Program Sponsor*** – Specific to EV Program sponsors. This includes program sponsor name; CEO name and contact information (e.g., telephone number, email address, physical/mailing address); and location and contact information (e.g., addresses, phone number).
- ***Case-Related*** – Specific to school officials and nonimmigrants. This includes number; adjudication determinations; site visit reports; appeals determinations; administrative reviews; and information pertaining to investigations, including results of searches of the Financial Crimes Enforcement Network systems or the National Crime Information Center.
- ***Auditing and Training*** – Specific to users of SEVP-owned systems. Includes auditing information (e.g., IP addresses, access and change history, date/time access, username, user role); system login (e.g., username, password, email address, name of individual,

unique identifiers such as SEVIS ID, IIN, and OPID); and training information (e.g., training status, training certificates, training transcripts).

- ***Reporting*** – Specific to F/M/J nonimmigrants, schools, and EV Program sponsors and their officials. Includes reporting information (e.g., aggregate data, statistics).
- ***Inquiries and Data Corrections*** – Specific to school officials and nonimmigrants. This includes contact information (e.g., telephone number, email address, physical/mailing address); unique identifier (e.g., SEVIS ID, IIN, OPID); identity documents (e.g., driver's license, passport, marriage certificate).

***Categories of Transactions***

ICE and DOS use the categories of information identified above for daily activities, as follows:

- ***Identity Validation*** – Biographical and identity verification information is used to identify and validate the identity of F/M/J nonimmigrants, school and program officials, and Federal Government personnel to ensure data integrity, accuracy, and proper data matching, as well as to authenticate individuals who either access SEVP systems or need to update information maintained by SEVP.
- ***Determination and Status*** – Biographical, school, program sponsor, immigration-related, and financial information is used to facilitate and support determination activities related to admissibility into the United States and the eligibility for and status of benefits.
- ***Adjudication*** – ICE uses school information to review and decide whether to certify a school, whereas DOS uses program sponsor information to designate a program so that F/M/J nonimmigrants may enroll or participate in the U.S.-based school or program. ICE also conducts criminal background checks on school officials to determine their suitability to participate in the program. Additionally, information from open-source media sites (e.g., publicly available information in newspapers, school websites, personal and organizational social media websites and blogs, government websites, and online forums) is used to support vetting of F/M/J nonimmigrants and their dependents and school and program officials who handle PII for F/M/J nonimmigrants and their dependents.
- ***Compliance*** – Biographical, identity verification, financial, travel, immigration-related, school, program sponsor, auditing and training, and reporting information is used to monitor F/M/J nonimmigrants, schools and programs, and their officials' compliance with immigration laws and regulations, including those addressing employment and training activities and immigration benefits, that govern (1) F and M

nonimmigrants and the schools that enroll or seek to enroll them through the SEVP certification process, and (2) participation of J nonimmigrants and programs with the EV Program.

- ***Investigative*** – Biographical, identity verification, education, program, employment, financial, travel, immigration-related, open-source information, and auditing and reporting information is used to perform administrative investigations. Administrative investigations are conducted to ensure that F/M/J nonimmigrants maintain their status and comply with U.S. laws and regulations. In addition, this information is shared with other government and law enforcement agencies for purposes of coordinating activities such as administrative reviews and criminal investigations.
- ***Analysis and Reporting*** – Biographical, education, program, school, program sponsor, financial, employment, travel, immigration-related, and reporting information is used to create and provide reports for analyzing compliance issues and identifying activities and related individuals (if needed) for evidence-based decision-making.[11]
- ***Communication and Customer Relations*** – Biographical, identity verification, school, program sponsor, case-related, and inquiry and data correction information is used to provide customer service to individuals who contact SEVP (e.g., via telephone, email, chat, SMS, social media), whether to provide information on SEVP regulations, perform data corrections, or provide technical support to access SEVP systems.[12]
- ***Training*** – Biographical, school, program sponsor, and training information is used to keep track of training activities performed by school and program officials in order to validate compliance with SEVP requirements to access SEVP external-facing systems.

***SEVP Systems***

SEVP systems collect, capture, and maintain information related to F/M/J nonimmigrants, the certified schools and EV Programs these individuals can attend, certified school and program officials, and employers with whom the nonimmigrants work. In addition, SEVP systems provide automated workflow capabilities, document repository, and electronic records management for SEVP records. These systems are used by Federal Government personnel, school and program officials, and F/M/J nonimmigrants.

SEVP has four external-facing systems that individuals outside of DHS may access. The first external-facing system is SEVIS, an Internet-based system that maintains real-time

[11] The SEVP Data Team, in conjunction with the SEVP Analysis and Operations Center (SAOC), performs and manages analysis and reporting activities, including trend and predictive analysis, for all SEVP data to support decision-making activities that include administrative reviews and support of investigations.
[12] EV Program–related inquiries or data correction requests are handled by DOS. If SEVP directly receives any of these inquires or requests, they are immediately transferred to DOS for appropriate handling.

information on F/M/J nonimmigrant students, their dependents, and school and program officials. School and program officials access the system to provide information about their school or program and the F/M/J nonimmigrants enrolled in their school or EV Program. ICE uses the information to monitor and track F/M/J nonimmigrants who have entered the United States and the compliance of F/M/J nonimmigrants and school and program officials.

The second external-facing system is the I-901 Fee Collection Services System (I-901 Fee System), an Internet-based financial management system that is responsible for collecting required fees from F/M nonimmigrants so they can enroll in a school or program.

The third external-facing system is the SEVP External Training Application (SETA), a Web application that is hosted in Amazon Web Services (AWS). SETA is a learning management tool that provides a single location to access training courses on a variety of topics to school and program officials.

The fourth external-facing system is Study in the States, a DHS website managed by SEVP that serves as an information resource for the international student community, tailored specifically to international students and SEVP-certified school officials. Study in the States helps students understand and comply with the rules and regulations that govern the international student process. Study in the States is supplemented with social media platforms (e.g., Facebook, Twitter) and other channels, such as conferences and events to communicate information to SEVP stakeholders.

Finally, the Student and Exchange Visitor Program Automated Management System (SEVPAMS), the I-515 system, and the Contact Center Communications and Management Suite (CCCMS) are used only by Federal Government personnel at SEVP and provide automated workflow capabilities, collaboration workspace, document repository, inquiry tracking, and electronic records management for SEVP records.

Please see Appendix B for detailed information on SEVP systems.

***Scenario: SEVP Collection and Use of Information***

To clarify how SEVP collects and uses information, a basic scenario related to certification of a school and enrollment of an F or M nonimmigrant student is provided below.

School Certification Process

A U.S.-based school seeking initial or continued authorization for attendance by nonimmigrant students must submit a petition to the SEVP School Certification Unit (SCU). The SCU certifies schools that want to enroll nonimmigrant F-1 (academic) and M-1 (vocational) students studying in the United States and adjudicates their initial, update, and recertification petitions. The school completes and submits Form I-17, "Petition for Approval of School for

Attendance by Nonimmigrant Student",[13] which includes information on designated school officials and supporting documents, for SEVP certification via SEVIS. The supporting documents are electronically transferred into SEVPAMS for SEVP to review.

As part of the adjudication process, SEVP, through its partnership with CTCEU, will run criminal background checks on school officials. In addition, the SEVP Field Representative Unit (FRU) conducts a site visit of the school. The FRU acts as the direct day-to-day liaison between SEVP and SEVP-certified schools who enroll nonimmigrants students. Information collected from the site visit is then added to SEVPAMS for review.

Once the adjudication process is complete, SCU issues a decision to approve or deny the certification. If denied, the school may appeal the decision. SCU will review all the information on the school maintained in SEVIS and SEVPAMS and issue a final decision. Once a school is SEVP-certified, the school may begin issuing Certificates of Eligibility (COEs), Form I-20,[14] for F or M admission to the United States. Finally, these school officials work with nonimmigrant students to enroll them in their school's programs, assist them with entry into the United States, and ensure they maintain compliance with the laws and regulations once they are in the country.

Nonimmigrant Application Process

A nonimmigrant seeking to study in the United States must apply to an SEVP-certified school. The SEVP-certified school is responsible for granting or denying student admission to the school, not SEVP. Once the student is granted admission, the school will create a student account in SEVIS and issue a COE, Form I-20, which allows the foreign student to enter the United States. The I-20 Form is sent via email to a personal email account provided by the student; students are also able to pick up the I-20 Form from a foreign Embassy/Consulate or other foreign offices (e.g., educational) if they prefer, but are then required to provide identity documents to an official before receiving the form.

Next, a prospective student seeking to enroll in a course of study at an SEVP-certified school must obtain an F-1 or M-1 nonimmigrant visa from DOS to enter the United States, fill out Form I-901, "Fee Remittance Form for Certain F, J and M Nonimmigrants,"[15] and pay the mandatory fee via the I-901 Fee System. The I-901 Fee System will automatically confirm the students name and fee amount via SEVIS before accepting payment and issuing a receipt. The F/M nonimmigrant must provide the I-20 Form and I-901 Fee system receiptat the time of arrival at a U.S. port of entry.

[13] U.S. Department of Homeland Security Form I-17, "Petition for Approval of School for Attendance by Nonimmigrant Student," OMB Control No. 1653-0038.
[14] U.S. Department of Homeland Security Form I-20, "Certificate of Eligibility for Nonimmigrant Student Status," OMB Control No. 1653-0038.
[15] U.S. Department of Homeland Security Form I-901, "Fee Remittance Form for Certain F, J and M Nonimmigrants," OMB Control No. 1653-0034.

If an F/M nonimmigrant arrives at a U.S. port of entry and does not have the required documentation (hereinafter, "documentary evidence"), a customs official will issue an I-515A Form, "Notice to Student or Exchange Visitor," which gives him or her temporary, lawful status for thirty days.[16] The customs official enters the I-515A Form into TECS (not an acronym),[17] which is maintained in the I-515 System and used to track the nonimmigrant's documentary evidence. If the nonimmigrant does not submit the required documentary evidence within thirty days, SEVP terminates the nonimmigrants status in SEVIS, and he or she must either leave the United States or apply for reinstatement. Once SEVP receives the documentary evidence, the record is closed in the I-515 System and stored in SEVIS and SEVPAMS.

***Privacy Safeguards***

This PIA explains how SEVP collects, shares, and manages personal information on individuals and describes the privacy protections implemented by SEVP to mitigate privacy risks. For example, SEVP has established Rules of Behavior that outline security and privacy requirements to access and use information within SEVP-owned systems. Federal employees must agree to follow the Rules of Behavior prior to accessing a system. In addition, administrative, physical, and technical access controls restrict access to information based on need to know. Finally, SEVP takes a holistic and proactive approach toward privacy by answering privacy questions from and providing training to SEVP personnel, as well as reviewing and assessing activities such as procurements, rulemakings, system development requirements, information collections, and information sharing at SEVP.

# Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal Government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of PII. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall ensure that information is handled in full compliance with the fair information practices set forth in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed the Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass DHS's full breadth and diversity of the information and interactions. The FIPPs account for the nature

[16] U.S. Department of Homeland Security Form I-515A, "Notice to Student or Exchange Visitor," OMB Control No. 1653-0037.
[17] See DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), *available at* https://www.dhs.gov/privacy.

and purpose of the information being collected relative to DHS's mission to preserve, protect, and secure.

DHS conducts PIAs on both programs and IT systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222. SEVP is a program rather than an IT system. In this section, the privacy impact of SEVP activities is examined as these activities relate to the FIPPs.

## 1. Principle of Transparency

*Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).*

General notice about the information collected, used, shared, and maintained by SEVP is provided by this DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP) PIA. In addition, the DHS/ICE-001 Student and Exchange Visitor Program (SEVP) System of Records Notice (SORN) applies to information collected and maintained in SEVP systems.[18]

In addition, information is collected directly from the individual, thereby making that person aware that his or her information will be used for specific purposes. For example, school and program officials also directly provide their own biographical information. This ensures that information provided is as accurate as possible. Similarly, information provided by school officials on F/M/J nonimmigrants is also collected directly from the student.

In some instances, SEVP information may be referred to CTCEU to investigate potential criminal and immigration violations (e.g., fraud by the school or visa fraud by a nonimmigrant). Notice to individuals in this regard is limited because providing notice to the subject of the record could undermine ICE's efforts to investigate leads, locate individuals, or take the appropriate enforcement actions. If any SEVP-related information is used for law enforcement or investigative purposes, individuals are not given notice or the opportunity to consent to avoid compromising an investigation or other ongoing law enforcement activity.

**Privacy Risk:** There is a risk that individuals may not be aware that their information may be contained within SEVP systems.

**Mitigation:** This risk is partially mitigated. The publication of this PIA and the corresponding SORN provides detailed descriptions of the types of individuals whose information is contained in SEVP systems, the data stored by SEVP systems, and how the information is used. In addition, Privacy Act statements (or privacy notices) provide information on ICE's authority to

[18] DHS/ICE-001 Student and Exchange Visitor Program (SEVP) SORN, *available at* www.dhs.gov/privacy. An updated SEVP SORN will be published concurrently with this PIA.

collect the information being requested, the purpose of the collection, notice that the information may be shared outside of DHS/ICE as permitted by federal law and policy, and whether the collection of information is mandatory or voluntary.[19] Privacy notices are posted on all SEVP systems and websites and made available to the individual at the time of collection. When it is not possible to provide written notice (e.g., phone call), SEVP provides verbal notice to inform individuals that they will need to provide personal information and where to locate the written privacy statement for the information collection. Finally, information is collected directly from the individual, thereby making that person aware that his or her information will be used for specific purposes at the time the information is being collected. For example, nonimmigrant students who elect to and receive approval for work study as Optional Practical Training (OPT) after completing their program use the SEVP Portal web application to enter and update contact and employment information.

## 2. Principle of Individual Participation

*Principle: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Individuals electing to enroll in a school that is SEVP-certified or participates in an EV Program constitutes consent. In order to participate in the SEVP program, individuals and entities (e.g., schools) are required to provide specific information and adhere to certain federal laws and regulations. Individuals are also given the opportunity to consent to the collection, use, dissemination, and maintenance of their PII when they provide information directly to ICE through the Office of Management and Budget (OMB)-approved information collections. These information collections are voluntary, and the notice provided to the individual during the collection explains the consequence of failing to provide the requested information (e.g., withdrawal of eligibility to enroll students).

Any individual, regardless of citizenship, seeking notification of and access to any of the records covered by this PIA may submit a request in writing to the ICE Freedom of Information Act (FOIA) officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009

[19] Privacy language is developed according to the DHS Privacy Policy Guidance Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information, *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

Washington, D.C. 20536-5009
Phone: (866) 633-1182
Fax: (202) 732-4266
Email: ICE-FOIA@dhs.gov
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act or the FOIA to prevent harm to law enforcement investigations or interests. Providing individuals with access to these records could inform the target of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interests 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.

The right to request an amendment of records under the Privacy Act of 1974[20] is limited to U.S. citizens and lawful permanent residents. Executive Order (EO) No. 13768, *Enhancing Public Safety in the Interior of the United States* (January 25, 2017), states the following: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies excludes persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[21] This EO precludes DHS from extending such rights to non-U.S. citizens or lawful permanent residents by policy. However, the Judicial Redress Act (JRA) of 2015 (5 U.S.C. §552a note),[22] which amended the Privacy Act, provides citizens of certain countries with access, amendment, and other redress rights under the Privacy Act in certain limited situations.[23]

As a result of EO 13768, DHS's "Mixed Systems Policy"[24] was rescinded by the DHS Privacy Office in its Privacy Policy Guidance Memorandum 2017-01 (April 25, 2017).[25] This changes

[20] 5 U.S.C. §552a.
[21] Executive Order No. 13768, *Enhancing Public Safety in the Interior of the United States* (January 25, 2017), https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.
[22] 5 U.S.C. §552a note.
[23] The foreign countries and regional organizations covered by the JRA, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the JRA, please visit the U.S. Department of Justice website at https://www.justice.gov/opcl/judicial-redress-act-2015.
[24] The "Mixed Systems Policy" extended most Privacy Act protections to visitors and aliens whose information was collected, used, maintained, or shared in connection with a mixed system of records (e.g., contains PII on U.S. citizens and lawful permanent residents, and non-U.S. citizens and non-lawful permanent residents). For more information *see* Memorandum Number 2007-1, *DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[25] DHS Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of

the ability of F/M/J nonimmigrants/aliens to access and correct their records maintained in a system of records at DHS, such as SEVIS or other SEVP systems. However, DHS Privacy Policy Guidance Memorandum 2017-01 reiterates that DHS/ICE has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate, relevant, timely, and complete records. Collecting, maintaining, using, and disseminating accurate information helps DHS to efficiently meet its operational goals, prevent waste, and improve outcomes. Failure to maintain accurate records undermines efficient decision-making by DHS personnel and can contribute to errors made by DHS and its personnel. To that end, the Privacy Division of the ICE Office of Information Governance and Privacy (IGP) accepts requests to amend from all individuals, regardless of citizenship. ICE may determine to make such corrections if there is no harm to law enforcement investigations or interests. All individuals can either submit these requests by email to ICEPrivacy@ice.dhs.gov or by mail to the following address:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy
ATTN: Privacy Division
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
Email: iceprivacy@ice.dhs.gov
http://www.ice.gov/privacy/

All or some of the information may be exempt from amendment pursuant to the Privacy Act (for those individuals who are not U.S. citizens or lawful permanent residents and whose records are not covered by the JRA) to prevent harm to law enforcement investigations or interests.

**Privacy Risk:** Individuals who are not U.S. citizens or lawful permanent residents, or who are not covered by the JRA, may have no avenue for redress or correcting records.

**Mitigation:** This risk is partially mitigated. SEVP has an independent operational need to ensure that F/M/J nonimmigrant data is accurate, relevant, timely, and complete. F/M/J nonimmigrants may contact their school or program official and correct or update their information maintained in SEVP systems. In addition, schools and nonimmigrants may contact the SEVP Response Center (SRC) directly and make a request to correct or update their information in SEVP systems. F and M nonimmigrants participating in Optional Practical Training (i.e., work study) create their own account in the SEVP Portal where they can provide and update their information

Personally Identifiable Information (April 25, 2017) (DHS Privacy Policy), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01. As the DHS Privacy Policy notes, EO 13768, does not affect statutory or regulatory privacy protections that may be afforded to foreign nationals, such as confidentiality rights for asylum seekers and refugees, and individuals protected under 8 U.S.C. §1367. These laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and foreign nationals, regardless of a person's immigration status.

directly. Finally, DHS/ICE has an obligation as a data steward, separate and apart from the Privacy Act, to maintain accurate and complete records. Therefore, F/M/J nonimmigrants may in some cases correct their records.

## 3. Principle of Purpose Specification

*Principle: DHS should specifically articulate the authority that permits the collection of PII and particularly the purpose or purposes for which the PII is intended to be used.*

ICE has been authorized to collect information by 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, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act); Public Law 107-173, Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act); 8 U.S.C. § 1372; 8 U.S.C. § 1761; 8 U.S.C. § 1762; 8 C.F.R. §§ 214.2(f), (j), and (m); 8 C.F.R. § 214.3; 8 C.F.R. § 214.4; 8 C.F.R. § 214.5; 22 C.F.R. Part 62; 8 C.F.R. § 214.12; 8 C.F.R. § 214.13; and Homeland Security Presidential Directive-2 (HSPD-2, Combating Terrorism Through Immigration Policies), as amended by HSPD-5, Management of Domestic Incidents, Compilation of HSPDs.

The information SEVP collects, captures, uses, shares, and maintains is handled in a manner consistent with the purposes necessary to perform and support the DHS, ICE, and SEVP missions. For SEVP, information collections are aligned with the relevant laws and regulations that support the ICE mission, and used for activities such as the following:

(1) Identifying individuals and validating their identity.

(2) Facilitating the admissibility determination for individuals seeking to enter the United States.

(3) Adjudicating schools and EV Programs as part of the certification and designation processes.

(4) Ensuring compliance with relevant laws and regulations by F/M/J nonimmigrants and schools and exchange visitor programs, including their officials, and the ability to act upon potential compliance violations.

(5) Investigating schools, EV Programs, school and program officials, and F/M/J nonimmigrants for unlawful activities such as fraud and terrorism.

(6) Analyzing and reporting data points related to activities such as overstays by F/M/J nonimmigrants, including trends and predictive analytics.

(7) Communicating and providing support for customer relations related to the SEVP program, including tracking inquiries related to SEVP and SEVP system technical issues from schools, EV Program sponsors, school and EV program officials, and F/M/J nonimmigrants.[26]

(8) Training purposes.

**Privacy Risk:** There is a risk that the information in SEVP systems is used for purposes beyond those described in this PIA.

**Mitigation:** This risk is partially mitigated. Federal Government personnel accessing SEVP systems are required to sign a Rules of Behavior document before accessing SEVP systems, confirming that they will protect sensitive information from disclosure to unauthorized persons or groups. For school and program officials accessing SEVIS, criminal background checks are conducted before SEVIS access is granted and a system warning notification is displayed when the users access reports in the system.[27] The following warning displays when authorized SEVIS users download a report from the system:

> *This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy related to FOUO information and is not to be released to the public or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official. This information shall not be distributed beyond the dhs.gov network without prior authorization of the originator.*

## 4. Principle of Data Minimization

*Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

SEVP collects and maintains pertinent information on nonimmigrant students and exchange visitors and their dependents, the schools and EV Programs and sponsors who enroll,

[26] On occasion, individuals from the public, such as members of Congress, the media, and attorneys for F/M/J nonimmigrants and schools or exchange visitor programs, may contact SEVP to ask about the program, SEVP regulations, and other topics related to SEVP.
[27] In the future, school and program officials with access to SEVIS may be required to undergo vetting and background investigations similar to those conducted for federal employees and contractors.

and school officials to ensure all parties comply with the laws and regulations that support SEVP's mission.

**Privacy Risk:** There is a risk that SEVP collects more information than is necessary for the purposes of the program.

**Mitigation:** ICE collects only a limited amount of information about individuals that is narrowly tailored to effectively and efficiently carry out the purposes of the program. ICE collects information from F/M/J nonimmigrants, school and program officials, and Federal Government personnel via paper-based, web-based, and other electronic forms (e.g., surveys, applications). All information collections must proceed through a formal information collection process of review and approval prior to use. ICE has established a Forms Management Program, Forms Management Policy, and other procedures to ensure efficiency, uniformity, and consistency in all forms management activities.

For example, IGP conducts a review to ensure that the data elements are compatible, relevant, and necessary to fulfill the collection's purposes. In addition, IGP confirms with the Office of the Principal Legal Advisor (OPLA) that ICE has the legal authority to collect the information before the form is approved. Any additions or modifications to the information collection(s) must proceed through the same formal process. Finally, these information collections must be reviewed; agreed to in writing by OPLA, IGP, SEVP, and NSID reviewing officials; and approved in writing by the Executive Associate Director of HSI.

For a comprehensive list of OMB-approved information collections maintained by SEVP, see Appendix A.

Furthermore, records retention schedules are generated, reviewed, and approved by the ICE Records Management Division and OPLA in conjunction with SEVP and the National Archives and Records Administration (NARA). The SEVP retention schedules are based on the administrative, fiscal, and legal value of the records, as well as privacy considerations.

**Privacy Risk:** There is a risk that information collected and maintained by SEVP is retained longer than necessary to accomplish the purpose for which it was originally collected.

**Mitigation:** This risk is partially mitigated. An SEVP program-wide, media-neutral records retention schedule is currently under development. Until a comprehensive schedule is in place, ICE will maintain these records permanently or in accordance with the appropriate NARA-approved general records schedules (GRS). For example, case files on school certification will be maintained for ten years. For SEVP financial management and reporting administrative records (e.g., audit information, system logins, inquiries, reporting), ICE will maintain the files for three years or longer if needed for business use. The GRS can be found at http://www.archives.gov/records-mgmt/grs.html.

## 5. Principle of Use Limitation

*Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

The sharing of SEVP information is aligned with the purpose for which the information is collected. SEVP shares information in five ways: (1) internally within SEVP; (2) internally within ICE; (3) internally within DHS and its components; (4) externally with other federal agencies; and (5) externally with nonfederal organizations.

**Privacy Risk:** There is a risk that data will be shared with external parties who do not have a need to know.

**Mitigation:** This risk is partially mitigated. All external sharing falls within the scope of published routine uses defined in the DHS/ICE-001 Student and Exchange Visitor Program (SEVP) SORN or follows DHS policy, including DHS Memorandum 2017-01 regarding the collection, use, retention, and dissemination of PII. In addition, Information Sharing and Access Agreements (ISAAs), such as a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), and other data sharing agreements, outline the purpose and scope of information sharing with external partners. These sharing agreements also play a central role in sustaining ICE's information and data governance practices providing the critical procedural controls necessary for effectively identifying and managing the risks of unauthorized use, uncontrolled sharing, and noncompliant information processes that may ultimately impact privacy, civil rights and civil liberties, and security mandates.

For example, ISAAs include a provision restricting a user who receives access to the system or information from the system from disseminating that information unless he or she has prior approval from ICE. Finally, ICE and SEVP periodically audit ISAAs and other data sharing agreements to ensure the external party complies and internal documentation is updated to reflect existing system interfaces and data sharing activities.

**Privacy Risk:** There is a risk that data may be used in a manner inconsistent with the original collection.

**Mitigation:** This risk is partially mitigated. SEVP has implemented administrative and technical access controls that help to ensure information maintained by SEVP is used according to the purposes identified in this PIA and other related notices. SEVP has role-based access controls, which are based on the individual's need to know the information and use it according to permitted purposes.[28] In addition, all Federal Government personnel are provided Rules of Behavior outlining the proper use of information in the system. The system users must agree to the Rules of

[28] Further details on access controls can be found in the Principle of Security section within this PIA.

Behavior, attesting that they will appropriately handle information maintained in any SEVP system before accessing information. At a minimum, users who fail to follow the Rules of Behavior or abuse their privileges may have their access to SEVP systems revoked. Depending on the type of user (e.g., Federal Government personnel, school and program official) and the nature of the violation, specific remedies may be implemented. If system administrators notice that any Federal Government personnel have used the system in violation of ICE policy, the incident will be referred to the appropriate agency internal affairs office for investigation. Finally, noncompliance, including inappropriate access and use, by Federal Government employees may be referred to the ICE Office of Professional Responsibility (OPR), when appropriate, for further action.

## 6. Principle of Data Quality and Integrity

*Principle: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete within the context of each use of the PII.*

SEVP ensures the quality and integrity of the data it collects, uses, shares, and maintains by obtaining information directly from the individuals who are the subjects of the data. This increases the likelihood that the information is accurate. School and program officials use SEVIS to create a student account and generate a COE for F/M/J nonimmigrants, which contains contact and biographical information provided by nonimmigrants. Similarly, school and program officials also directly provide their own biographical information. For data received from other agencies, it is the original data collector's responsibility to ensure the accuracy of information provided to SEVP.

**Privacy Risk:** There is a risk that the entity or nonimmigrant may not be aware that the information maintained in SEVP systems is incomplete or SEVP systems could contain inaccurate information.

**Mitigation:** This risk is partially mitigated. SEVP closely monitors record-keeping procedures and reporting requirements during the SEVP certification and recertification process. For school certifications, if inaccurate data is identified, or adverse information is discovered or reported by a third party, SEVP informs the provider and school officials what information is incorrect and what steps the individual can take to correct it. In addition, schools can submit a final appeal if they do not agree with a decision.

For information provided on F/M/J nonimmigrants by third parties (e.g., school or program officials, Federal Government personnel, other Federal Government systems), F/M/J nonimmigrants are instructed to review their COE for inaccuracies and either contact the school or program official assigned to them or contact the SRC to request data correction. The SRC serves as the single point of contact for all SEVP stakeholders, including nonimmigrants and school and program officials.

School and program officials review the information provided and may request documentation to verify its accuracy, including employment information. If the school or program official is unable to correct an F/M/J nonimmigrant's information directly within a SEVP system, then the official may contact SEVP and go through the data-correction process. This process involves identifying the type of corrections needed, providing evidence validating that the data given to SEVP is accurate, and ensuring that the appropriate changes are made. This process will help reduce the risk of having inaccurate or fraudulent data in SEVP systems. Finally, general instructions can be found online in the Study in the States website.

## 7. Principle of Security

*Principle: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

SEVP has implemented several administrative, physical, and technical safeguards to protect SEVP systems and the information collected and maintained in SEVP systems. All administrative, physical, and technical safeguards are based on the principle of "need to know."

**Privacy Risk:** There is a privacy risk that SEVP information may be accessed by unauthorized individuals.

**Mitigation:** This risk is partially mitigated. Access to SEVP facilities is limited to federal employees and contractors. In addition to physical security, SEVP's policy is based on the principle of need to know, which also applies to system access controls. Individuals cannot access the systems without an account created by the system administrator. Only system administrators can make changes to the system and grant access to other authorized users.

As a federal database, SEVIS is subject to the Federal Information Security Modernization Act (FISMA), which requires the annual verification that all users who access federal systems have both the business need and the authorization to access the system. To comply with FISMA, school officials, officers, and government users must annually verify employment and their role requires continued access to SEVIS. System administrators will terminate access for federal government personnel no longer employed by SEVP and public users (e.g., school and program officials).

SEVP uses technical access controls to ensure that only authorized users can access the data in the system. Additionally, role-based access is used to limit users' access to the information necessary for their positions, which ensures technical access controls comply with the need-to-know principle. Certain Federal Government user groups may only have "read-only" access to specific information types, while other groups have read/write/edit privileges. This is based on users' roles and responsibilities and implemented by system administrators

SEVP systems maintain audit logs of user activity, including system administrator accounts (i.e., ICE personnel) to monitor unusual system behavior. Audit reports are reviewed by SEVP, ICE, and DHS, which allows for multiple levels of review to identify misuse of system access. Audit logs track when individuals are logged onto the system, who views which records, and how records are used within the system (e.g., unauthorized creation, system configurations). Audit records are detailed enough to reconstruct records if a system is compromised or a system malfunction occurs. Audit logs allow ICE personnel to track external disclosures and ensure the information is being shared in accordance with the provisions of this PIA and applicable SORN.

Finally, under the terms of ISAAs, external parties agree to secure the information consistent with approved security practices that meet DHS standards. External parties agree that personal information will be kept secure and confidential and will not be divulged to any person without an official need to know. This includes the physical, technical, and administrative safeguards mentioned above.

## 8. Principle of Accountability and Auditing

*Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Training

Education is a significant step in helping to ensure information maintained by SEVP is used appropriately. Some of the most important concepts taught are the FIPPs, especially when discussing and making decisions on information collections and capture, purpose, and use of the information, and how to mitigate the risks. Privacy education has been beneficial because it increases knowledge of laws and regulations on PII and Sensitive PII in general and identifies the various limitations on how information maintained by SEVP may be used and shared. Privacy teaches that a proactive approach to assessing privacy risks and actions to mitigate risks yields benefits such as risk reduction as well as improved products, systems, services, and cost impact.

Annual mandatory security and privacy training is completed by all Federal Government personnel. The training provides agency requirements on handling information in various formats, including paper and electronic. Individuals may have their access to ICE systems revoked if they do not complete their required training. In addition, internal instructions are made available to authorized federal government personnel located at DHS, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), and DOS on the access and use of internal SEVP systems. For external parties who access SEVP systems, step-by-step instructions and demos are available at www.StudyintheStates.dhs.gov. Additionally, new privacy and security

training is under development and will fill a gap for external system users, providing knowledge and outlining consequences for misuse of the information in SEVP systems. This training will be made available to external users with access to SEVP systems. Possible consequences for school and program officials' misuse of information could be the removal of the SEVP system access, withdrawal of the school's SEVP certification to enroll F/M nonimmigrant students, or revocation of the EV Program's DOS designation as an authorized program sponsor.

Auditing

SEVP systems are regularly audited to ensure that systems are being used appropriately and in accordance with privacy and security requirements. Auditing SEVP systems is a shared responsibility among DHS, the ICE Chief Information Security Officer (CISO), and ICE Information System Security Officers (ISSOs). All are responsible for coordinating, implementing, and managing technology security regulations and requirements, including actively reviewing system security logs to identify threats to the systems. ICE has several mechanisms in place to ensure that its systems and information are used appropriately.

SEVP systems have a robust auditing feature that helps to identify and support accountability for user misconduct. SEVP system users are provided notice before accessing the system and that their use is monitored during system training. Suspicious or unauthorized access is monitored and logged, thereby discouraging users from inappropriate access to SEVP systems. ISSOs perform routine reviews to monitor security (e.g., disablement of security, login times, number of login attempts, failed login attempts) and check for misuse (e.g., unauthorized removal of data) by authorized users, including system administrators. Audit logs are reviewed and reported to the ICE CISO on a regular basis by the ISSO. When unusual activity is detected within the system, the audit logs are used for incident investigations and determinations.

ISSOs routinely monitor misuse of the systems and may revoke access to SEVP systems or those who abuse their privileges; violations may also be reported to law enforcement. If system administrators notice that any federal employee has used the system in violation of ICE policy, the incident will be referred to the appropriate agency's internal affairs office for investigation. That federal employee will be disciplined according to his or her agency policy, which could include adverse actions or removal from federal service. For nonfederal users of SEVP systems, unauthorized or improper use or access of the systems may result in disciplinary action, as well as civil and criminal penalties. If there are unexplained system events that raise suspicion for possible further investigation, then the ICE CISO is notified.

Finally, program audits of SEVP may also be conducted by compliance officers within DHS and ICE, such as the DHS Office of the Inspector General. These audits typically examine whether the program office is proactively identifying and managing financial and operational risk. In addition to audits DHS internal audits, external federal parties, such as the Government Accountability Office (GAO) also periodically audits SEVP activities.

## Responsible Officials

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

## Approval Signature

[Original signed and on file with the DHS Privacy Office]

_____

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

# Appendix A
# OMB-Approved Information Collections/Forms

The following table provides a complete list of forms, approved by OMB, that collect information covered by the Paperwork Reduction Act (PRA). The information collected is used, shared, and maintained by SEVP.

| Category of Individuals Whose Information is Collected | Form Used to Collect Information |
|---|---|
| **F and M Nonimmigrants** | **U.S. Department of Homeland Security Form I-20, "**Certificate of Eligibility for Nonimmigrant Student Status," OMB Control No. 1653-0038<br><br>**U.S. Department of Homeland Security Form I-901,** "Fee Remittance Form for Certain F, J and M Nonimmigrants," OMB Control No. 1653-0034<br><br>**U.S. Department of Homeland Security Form I-983,** "Training Plan for STEM OPT Students. Science, Technology, Engineering & Mathematics (STEM) Optional Practical Training (OPT)," OMB Control No. 1653-0054<br><br>**U.S. Department of Homeland Security Form I-765**, "Application for Employment Authorization," OMB Control No. 1615-0040<br><br>**U.S. Department of Homeland Security Form I-539**, "Application to Extend/Change Nonimmigrant Status," OMB Control No. 1615-0003<br><br>**U.S. Department of Homeland Security Form I-94**, "Arrival/Departure Record," OMB Control No. 1651-0111<br><br>**U.S. Department of Homeland Security Form I-515A**, "Notice to Student or Exchange Visitor," OMB Control No. 1653-0037 |
| **J Nonimmigrants** | **U.S. Department of State Form DS-2019,** "Certificate of Eligibility for Exchange Visitor (J-1) Status," OMB Control No. 1405-0119<br><br>**U.S. Department of State Form DS-7002, "**Training/Internship Placement Plan," OMB Control No. 1405-0170<br><br>**U.S. Department of Homeland Security SEVIS Form I-901,** "Fee Remittance Form for Certain F, J and M Nonimmigrants," OMB Control No. 1653-0034<br><br>**U.S. Department of Homeland Security Form I-765**, "Application for Employment Authorization," OMB Control No. 1615-0040<br><br>**U.S. Department of Homeland Security Form I-539**, "Application to Extend/Change Nonimmigrant Status," OMB Control No. 1615-0003<br><br>**U.S. Department of Homeland Security Form I-94**, "Arrival/Departure Record," OMB Control No. 1651-0111<br><br>**U.S. Department of Homeland Security Form I-515A**, "Notice to Student or Exchange Visitor," OMB Control No. 1653-0037 |
| **Schools** | **U.S. Department of Homeland Security Form I-17,** "Petition for Approval of School for Attendance by Nonimmigrant Student," OMB Control No. 1653-0038 |
| **Exchange Visitor Program Sponsors** | **U.S. Department of State Form DS-3036, "**Exchange Visitor Program Application," OMB Control No. 1405-0147 |

| Category of Individuals Whose Information is Collected | Form Used to Collect Information |
|---|---|
| | **U.S. Department of State Form DS-3037,** "Update of Information on Exchange Visitor Program Sponsor," OMB Control No. 1405-0147<br><br>**U.S. Department of State Form DS-3097,** "Annual Report, J-1 Exchange Visitor Program," OMB Control No. 1405-0151 |

# Appendix B

# SEVP Systems

B1 – Student and Exchange Visitor Information System (SEVIS) and Subsystems

B2 – SEVP External Training Application (SETA) System

B3 – I-901 Fee Collection Services System

B4 – Study in the States

B5 – Contact Center Communications and Management Suite (CCCMS)

B6 – Student and Exchange Visitor Program Automated Management System (SEVPAMS) and Modules

# Appendix B1

# Student and Exchange Visitor Information System (SEVIS) and Subsystems

**Purpose and Use:**

The Student and Exchange Visitor Program (SEVP) is the owner of the Student and Exchange Visitor Information System (SEVIS), which is an Internet-based system that maintains real-time information on nonimmigrant students (F-1 and M-1 classes of admission), exchange visitors (J-1 class of admission), and their dependents (spouse and/or minor children in the F-2, M-2, and J-2 classes of admission).

The Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996 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 nonimmigrants are in the country, where they are, and what they are studying. After the September 11, 2001 attacks, 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 Department of State (DOS) deployed SEVIS in 2003 as the system of record for information on schools and exchange visitor program sponsors, their officials, and F/M/J nonimmigrants. SEVIS supports tracking and monitoring of F/M/J nonimmigrants and their 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 primarily from F/M/J school and exchange visitor program officials through SEVIS. F/M/J nonimmigrants can provide contact and employment information through their school and exchange visitor program officials, who have access to SEVIS. Information reported includes, but is not limited to, change of domestic address, changes in program study, and employment information, if applicable.

Finally, SEVIS collects and maintains information on school and program officials and allows schools to submit school certification applications, update certification information, submit updates that require adjudication, and create and update F/M/J student and dependent records.[29]

**Category of Transaction:**

- Identity Validation
- Determination of Status
- Adjudication
- Compliance
- Investigative
- Analysis and Reporting

[29] In the future, nonimmigrant students may be able to provide updated information using the SEVP OPT Portal.

- Communication and Customer Relations
- Training

**Category of Users with System Access:**[30]
- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- School Officials
- Program Officials
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- Schools
- School Officials
- Exchange Visitor Program Sponsors
- Program Officials
- Host Families
- Financial Support Provider
- Employers
- Federal Government Personnel

**Sources of Information:**
- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- School Officials
- Program Officials
- Federal Government Personnel
- Federal Government Systems

**Category of Information in the System:**
- Biographical
- Identity Verification
- Education
- Program
- Employment
- Financial
- Travel
- Immigration-Related
- School
- Program Sponsor
- Case-Related
- Auditing and Training
- Reporting
- Inquiries and Data Corrections

[30] For information on system access controls and other system safeguards, please see Section 7, Principle of Security.

## SEVIS Subsystems:

***SEVIS Admissibility Indicator (SEVIS-AI)***

The SEVIS Admissibility Indicator (SEVIS-AI) Service is an internal-facing web service that transmits select SEVIS data and admissibility indicators, determined by regulation-based business rules, to U.S. Customs and Border Protection's (CBP) TECS system (not an acronym).[31] The SEVIS-AI subsystem does not return any information to the primary SEVIS system. SEVIS-AI helps support admissibility decisions for F/M/J classes of admission at the primary inspection point. When SEVIS records support a decision to admit, SEVIS generates a record that updates SEVIS-AI supporting a decision for admissibility. When SEVIS records show an issue that requires referral of the nonimmigrant to CBP secondary inspection, SEVIS-AI generates an admissibility indicator consisting of a reason code and narrative description. SEVIS-AI sends admissibility indicators to CBP only upon receiving a TECS query from an officer at the primary inspection point. CBP stores limited SEVIS and admissibility data in the TECS database and makes this data available to officers at secondary inspection.

SEVIS-AI is intended to (1) streamline the process of furnishing SEVIS information to CBP; (2) reduce the reliance on paper documents for making admission decisions; (3) provide a way of assessing the current SEVIS data against the current regulatory requirements for admission as an F/M/J nonimmigrant; and (4) assist CBP officers in making faster, more informed decisions that greatly reduce the risk of fraudulent entry.

**Category of Transactions:**
- Identity Validation
- Compliance
- Determination and Status

**Category of Users with Access:**
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants

**Sources of Information:**
- Federal Government Systems

**Category of Information:**
- Biographical
- Auditing
- Identity Verification
- Reporting

[31] TECS is the updated version of the former Treasury Enforcement Communications System. See DHS/CBP/PIA-021 TECS System: Platform (August 12, 2016), *available at* www.dhs.gov/privacy.

***SEVP Professional I-515 Tracking System (formerly known as SPITS)***

I-515A is an internal-facing tracking system used to analyze, adjudicate, track, and manage the actions and evidentiary requirements from F/M/J nonimmigrants and dependents as part of the Form I-515A instructions. When F/M/J nonimmigrants lack proper documentation at a U.S. port of entry (e.g., they forgot their Certificate of Eligibility or are in non-active SEVIS status), they are referred to a secondary inspection, where CBP conducts vetting checks. If they are deemed suitable for entry, CBP issues a Form I-515A, which gives them temporary, lawful status and 30 days to satisfy the requirements listed on the form and submit evidence to SEVP. The I-515A system automatically generates an email notification to students and/or school or program officials informing them that SEVP must receive the original Form I-515A and required documents before the 30-day period expires to be granted an extension of stay for the study program's duration. Once all requirements are met, the I-515A record is closed and maintained in the I-515 system. If the documentation is not received in time, SEVP terminates F/M/J nonimmigrants' status in SEVIS and they must either leave the United States or apply for reinstatement to the United States Citizenship and Immigration Services.

**Category of Transactions:**
- Compliance

**Category of Users with Access:**
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants

**Sources of Information:**
- F and M Nonimmigrants
- J Nonimmigrants
- Federal Government Personnel
- Federal Government Systems

**Category of Information:**
- Biographical
- Identity Verification
- Auditing
- Reporting

***SEVP Information Sharing Interface (ISI)***

SEVIS shares and exchanges information with various federal information technology systems,[32] both internal and external to DHS. The SEVP ISI serves as an application programming interface for SEVIS. The SEVP ISI provides security and manages all system-to-system communications and data exchanges between SEVIS and internal and external interface partners. The SEVP ISI is a pass-through system, meaning the information is exchanged between SEVIS and the other federal systems but is not saved in the SEVP ISI. Data received is refreshed on a regular basis in accordance with the source system's schedule. In addition, the ISI ensures there is an efficient, accurate data transaction between systems because the interface aligns the data fields from the federal systems with those used by SEVIS.

The SEVP ISI allows SEVIS to be entirely separate from other systems. Exchanging data using SEVP ISI removes the risks associated with making changes directly within SEVIS and avoids any issues of overloading SEVIS and causing the system to become unavailable. The SEVIS ISI has auditing functionality that captures information on data exchanges for information security purposes.

**Category of Transactions:**

- Identity Validation
- Determination and Status
- Adjudication
- Compliance
- Investigative
- Analysis and Reporting
- Communication and Customer Relations
- Training

**Category of Users with Access:**

- Federal Government Personnel

**Category of Individuals Impacted:**

- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- Schools
- School Officials
- Exchange Visitor Program Sponsors
- Program Officials
- Host Families
- Financial Support Provider
- Employers
- Federal Government Personnel

**Sources of Information:**

- Federal Government Personnel
- Federal Government Systems

[32] For example, SEVIS is connected to the ICE Counterterrorism and Criminal Exploitation Unit (CTCEU) LeadTrac system and shares information on F and M students who are suspected of overstaying for further investigation. SEVIS is also connected to the DOS Consular Consolidated Database (CCD) and shares information on J exchange visitors and program sponsors and officials, thereby providing DOS with oversight of its Exchange Visitor Program. For more information on the CCD PIA, please visit https://www.state.gov/privacy-impact-assessments-privacy-office/; and for more information on the CCD SORN, please visit https://www.state.gov/system-of-records-notice-final-rules/.

**Category of Information:**

- Biographical
- Identity Verification
- Education
- Program
- Employment
- Financial
- Travel
- Immigration-Related
- School
- Program Sponsor
- Case-Related
- Auditing
- Reporting

***Analysis & Reporting Module***

SEVP uses Tableau to conduct analysis and reporting. Federal Government personnel use SEVIS information to enable evidence-based decision-making. Depending on the user's role, SEVIS reports may provide only statistical information or lists of individuals on whom some action needs to be taken. Aggregate data reports are specifically created for federal personnel, especially for investigation purposes. Typically, these reports are sourced from multiple systems, primarily from within DHS, although public information may also be combined with SEVIS data to provide useful reports for administrative compliance reviews and investigative purposes related to national security and public safety. Reports are also created when there are data calls by DHS and its components and other agencies, congressional inquiries, and Freedom of Information Act (FOIA) requests.

**Category of Transactions:**
- Analysis and Reporting

**Category of Users with Access:**
- Federal Government Personnel
- School Officials
- Program Officials

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- Schools
- School Officials
- Exchange Visitor Program Sponsors
- Program Officials
- Host Families
- Financial Support Provider
- Employers
- Federal Government Personnel

**Sources of Information:**
- Federal Government Personnel
- Federal Government Systems

**Category of Information:**
- Biographical
- Identity Verification
- Education
- Program
- Employment
- Financial
- Travel
- Immigration-Related
- School
- Program Sponsor
- Case-Related
- Auditing
- Reporting

***SEVP Portal – Optional Practical Training (OPT)***

The SEVP Portal is an external-facing web application that is used to manage and keep track of F and M nonimmigrant students who have been granted OPT or Practical Training work permission by USCIS. F and M nonimmigrant students studying in the United States have an opportunity to gain practical work experience in their field of study. Rather than relying on school officials to update this information on their behalf, F and M nonimmigrants can create an account through the OPT web application and directly provide their employment information. In the future, modifications to SEVIS may be made to expand the capability and use of the OPT Portal to allow/permit F and M nonimmigrant students to directly review and edit their biographical and contact information (except for their name, SEVIS ID, date of birth, country of birth and citizenship, gender, and email address).

**Category of Transactions:**
- Identity Validation
- Compliance

**Category of Users with Access:**
- F and M Nonimmigrants
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants

**Sources of Information:**
- F and M Nonimmigrants
- Federal Government Personnel
- Federal Government Systems

**Category of Information:**
- Biographical
- Identity Verification
- Auditing
- Reporting

# Appendix B2

# SEVP External Training Application (SETA) System

**Purpose and Use:**

***SEVP External Training Application (SETA)***

SETA is an external-facing learning management tool that provides training for school and program officials. SETA offers training courses on a variety of topics, including information related to the SEVP program, SEVP and DOS regulations, requirements for school certification and exchange visitor program designation, and practical training.

**Category of Transactions:**

- Training

**Category of Users with Access*:***

- School Officials
- Program Officials

**Category of Individuals Impacted*:***

- F and M Nonimmigrants
- J Nonimmigrants
- Proxy, Parent, or Legal Guardian
- School Officials
- Program Officials
- Federal Government Personnel

**Sources of Information:**

- Federal Government Personnel
- Federal Government System

**Categories of Information:**

- Auditing and Training
- Reporting

# Appendix B3

# I-901 Fee Collection Services System

**Purpose and Use:**

The I-901 Fee Collection Services System (I-901 Fee System or website) is an external-facing, Internet-based system that allows SEVP to collect information electronically from nonimmigrant foreign SEVP participants during their stay and to permit legitimate foreign students or exchange visitors to enter the United States. SEVP requires students and exchange visitors to register with SEVP by submitting Form I-901, along with the required fee, to the Financial Management Service (FMS), a bureau of the U.S. Department of the Treasury, via lockbox[33] (i.e., by mail) or the I-901 Fee System located on the I-901 Fee website. Approved Exchange Visitor Sponsoring Organizations also may submit Forms I-901 to ICE on behalf of multiple students and exchange visitors via bulk filing through the I-901 Fee website. More than 1,000,000 students and 8,700 schools annually use the I-901 Fee System to submit the I-901 fee payments to FMS. A contracted financial institution currently hosts the domains of www.fmjfee.com and www.fmjadmin.com (the I-901 Fee System). Previously, FMS managed the I-901 Fee System. FMS is still responsible for collecting the fees and for their proper disposition.

The I-901 Fee System comprises the following components to support payment of the I-901 fee:

1. A web-based payment system whereby a contracted financial institution hosts an Internet-based electronic version of the I-901 Fee Transmittal Form. This allows an individual to file the Form I-901 and pay the I-901 fee through a credit card interface to FMS's Pay.Gov credit card portal.

2. A lockbox payment mechanism whereby a person can mail a completed Form I-901 and associated payment to a lockbox hosted by the contracted financial institution.

3. A bulk filing capability whereby authorized Exchange Visitor Programs can upload a file of exchange visitor data and charge the payment via an Automated Clearing House debit to a predetermined sponsor bank account.

4. A Western Union payment mechanism whereby a person can remit the I-901 data and associated payments at a local Western Union office.

The I-901 Fee System involves interactions among DHS ICE SEVP, FMS, and the contracted financial institution to complete I-901 fee transactions. Payments received from F, M,

[33] A lockbox is a bank-operated mailing address to which a company directs its customers to send their payments. The bank opens the incoming mail, deposits all received funds in the company's bank account, and scans the payments and any remittance information.

and J nonimmigrant applicants are validated against SEVIS records to ensure that the payment is posted to the appropriate SEVIS record and that the applicant is given proper credit for having paid the required I-901 fee. Additionally, the validation with SEVIS is used to accurately identify individuals for visa issuance and entry into the United States.

The contracted financial institution, an SEVP contractor, serves as an agent for the government to administer, host, manage, and operate the I-901 fee site. The contracted financial institution also provides support services to the I-901 Fee System by processing Form I-901 applications and I-901 fee payment transactions. It also supports reporting capabilities, applicant inquiry and status information, applicant information updates, and financial reconciliation.

**Category of Transactions:**
- Compliance

**Category of Users with System Access:**[34]
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants

**Sources of Information:**
- F and M Nonimmigrants
- J Nonimmigrants

**Category of Information in the System:**
- Biographical
- Identity Verification
- Financial
- Auditing
- Reporting

[34] For information on system access controls and other system safeguards, please see Section 7, Principle of Security.

# Appendix B4
# Study in the States

**Purpose and Use:**

Study in the States, a DHS public website managed by SEVP, is a dynamic information resource for international students and SEVP-certified school officials to help them understand and comply with the rules and regulations that govern the international student process. Study in the States assists SEVP in educating the public and clearly articulates the U.S. Government's mission and policy to current and prospective foreign nationals and exchange visitors. SEVP uses feedback tools, such as surveys, feedback forms, and polls on the information and training provided on Study in the States, to help improve the information it presents to users of the website.

In addition, Study in the States enables schools to track the progression of their certification process, as well as progression of the appeals process. Using this feature, schools are assigned a unique identification number and staff can see which step in the SEVP certification or appeals process its case is currently undergoing, a basic description of that step, and the estimated length to complete. Staff who use the tracker see the same description used for each step in the certification or appeals process.

Study in the States has a blog and social media tools, such as Twitter, Facebook, LinkedIn, YouTube, RSS feed, and widgets (e.g., a small web application embedded on public websites or blogs that allows quick access to the Study in the States website) that serve as ways for the Federal Government to have a two-way dialogue and a one-way informational interaction with stakeholders across the international academic community. As a public-facing website, no registration is required to view the content provided through the social media tools and blog. However, for social media tools that allow for two-directional communication, such as the Study in the States's Facebook and Twitter accounts, these accounts can allow for the public to post comments, comment on the content, repost content, and "fan" the Study in the States/SEVP social media tool sites. This activity is allowed only if the user is registered to the social media tool.

Finally, some accounts (Study in the States's Facebook and Twitter accounts) receive inquiries through direct messages on both accounts and have a set of preapproved automatic responses that SEVP uses to respond. SEVP is pursuing the use of a chatbot to automate responses to questions received via Facebook. The chatbot will allow SEVP to automate responses to frequently received questions; however, no case-specific details are provided. If a case-specific question is submitted, the chatbot will provide contact information directing the individual to call the SEVP Response Center. Users are required to have an active Facebook account that has "liked" the Study in the States Facebook page to interact with the chatbot, and the chatbot then provides users with a disclaimer and prompts them to agree before the interaction. Other social media accounts, such as the Study in the States LinkedIn account, are used to provide outbound updates

only to school officials.

**Category of Transactions:**
- Communication and Customer Relations

**Category of Users with Access:** [35]
- F and M Nonimmigrant Students
- J Nonimmigrant Students
- Proxy, Parent, or Legal Guardian
- School Officials
- Program Officials
- Federal Government Personnel
- Members of the Public[36]

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants
- Schools
- School Officials
- Exchange Visitor Program Sponsors
- Program Officials
- Federal Government Personnel
- Members of the Public

**Sources of Information:**
- Federal Government Personnel

**Category of Information in the System:**
- Case-Related[37]
- Auditing and Training[38]
- Reporting

[35] For information on system access controls and other system safeguards, please see Section 7, Principle of Security, in this PIA.
[36] On occasion, individuals from the public, such as members of Congress and attorneys for F/M/J nonimmigrants, will access Study in the States to gain more information about SEVP.
[37] Specific case information is not made available via Study in the States. However, identifiers for specific transactions are provided for schools or individuals to keep track of pending activities. For example, an appeals tracker is used by schools to see where the status of their school certification appeals case at any time. An appeals number is provided to the school, and the school enters the number into the appeals tracker page. Template language provides where the school is in the appeals process. No additional information about the case is provided.
[38] Training materials are available via Study in the States; however, tracking of training for access to SEVIS is maintained in the SEVIS training module.

# Appendix B5
# Contact Center Communications and Management Suite (CCCMS)

**Purpose and Use:**

SEVP communicates to a wide audience, including students and school officials, congressional members and staff, agency partners, the public, and the Federal Government,[39] using different channels and formats (e.g., web, social media, conferences, email communications). The Contact Center Communications and Management Suite (CCCMS) is a Voice over Internet Protocol internal-facing system that provides a unified communication and management system and suite of tools to provide interactive services by tracking and effectively managing the workflow of inquiries (e.g., received via emails, telephone calls, social media) managed by the SEVP Response Center (SRC).

These inquiries are related to both general questions and technical issues identified by external stakeholders, including Federal Government personnel, school and program officials, F/M/J nonimmigrants, and members of the public (e.g., attorneys, members of Congress). The SRC provides a personalized experience for the stakeholder, especially when handling a situation that is more sensitive (e.g., related to personal data or access to SEVP systems) and would require authentication of the individual prior to discussing or disclosing information from SEVP. The SRC also manages requests to SEVP from school officials to change data in SEVP systems.[40] The SRC manages and tracks these general inquiries, data change requests, and technical issues using SEVPAMS.[41] The SRC also authenticates callers, depending on caller type (e.g., F/M/J nonimmigrant, school/program official, Federal Government personnel) against SEVIS information, which is especially necessary for data change requests and technical help for SEVIS access.

CCCMS has various functions and tools that SRC customer service representatives (CSRs) and managers can use to provide effective customer service. These tools and functions include the following:

- The callback assistance tool gives callers the option of an immediate callback when an SRC CSR becomes available or a callback at a scheduled date and time.
- The recording function enables SRC management to record and archive telephone calls and record screen interactions between CSRs and stakeholders during calls and social media

[39] SEVP directs all Exchange Visitor Program communication (includes communication with J nonimmigrants, Exchange Visitor Program sponsors, program officials) to DOS for proper handling and accurate Exchange Visitor Program information.
[40] Please see Appendix B1 for more information on SEVIS.
[41] Please see Appendix B6 for more information on SEVPAMS.

interactions, thereby providing a remote view of on-screen activity for quality control monitoring and CSR training purposes. CSRs provide a verbal privacy notice to individuals during all telephone call interactions and screen interactions to warn users that calls may be recorded.

- The email function is used to send and receive inquiries from stakeholders (e.g., school and program officials, F and M students, members of the public), as well as receive documentation related to school official requests to change data in SEVIS.
- Administrative tools are used for internal operational forecasting and scheduling by management, including determining appropriate staffing needs during peak and low call volume times, thereby optimizing SRC's efficiency and customer communications.

**Category of Transactions:**
- Communication and Customer Relations

**Category of Users with System Access:**[42]
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- J Nonimmigrants
- Schools
- School Officials
- Exchange Visitor Program Sponsors
- Program Officials
- Federal Government Personnel
- Members of the Public[43]

**Sources of Information:**
- Federal Government Personnel
- F and M Nonimmigrants
- J Nonimmigrants
- School Officials
- Program Officials
- Members of the Public

[42] For information on system access controls and other system safeguards, please see Section 7, Principle of Security.
[43] On occasion, individuals from the public, such as members of Congress and attorneys for F/M/J nonimmigrants, will access Study in the States, SEVIS, and ICE.gov to get more information about SEVP.

# Appendix B6

# Student and Exchange Visitor Program Automated Management System (SEVPAMS)

**Purpose and Use:**

SEVPAMS is an internal SEVP system that provides automated workflow capabilities, a collaboration workspace, document repository space, inquiry tracking, and electronic records management. SEVP uses SEVPAMS to maintain documentation received from SEVP stakeholders (i.e., F/M nonimmigrants and school officials) to substantiate information entered into SEVIS. SEVP stakeholder documentation stored in SEVPAMS is related to SEVIS and SEVIS subsystem submissions, such as school certification and Form I-515A compliance. The workflows SEVPAMS provides allow SEVP units to complete mission tasks more quickly, such as SEVP field representative reports, adjudication processes, and communication with external stakeholders.

SEVPAMS is also used to maintain tips related to potentially noncompliant activities by schools, their officials, and F/M nonimmigrants. Tips are entered and tracked by SEVP personnel, who may have may receive them directly from members of the public, F/M nonimmigrants, or school officials. With its tracking functionality, SEVPAMS is used to track and record operational activities, including software and system service requests. SEVPAMS is used to process requests by Federal Government personnel who submit requests and documentation to access SEVIS.

SEVPAMS receives data from SEVIS to support school certification adjudication activity, such as tracking and managing school and official's information for initial certification, recertification, petition updates, and adjudication decision appeals. SEVPAMS has a bidirectional connection with SEVIS with a near-real-time exchange of status updates and information related to tracking and managing correction requests by school officials to correct F/M nonimmigrant data in SEVIS and receiving documents that have been uploaded through SEVIS. The interconnection between SEVIS and SEVPAMS allows school officials to use SEVIS to submit petition-related documents through SEVIS as a pass-through system[44] to a document repository in SEVPAMS. This interconnection allows SEVPAMS to securely route documents directly to their correct petition workspaces for the adjudication process. SEVPAMS also allows for various reports produced by SEVIS's Analysis & Reporting Module to be viewed from the SEVPAMS interface.

**Category of Transactions:**

- Identity Validation
- Determination and Status

[44] Documents intended for uploading via SEVIS are subject to a virus scan and must pass this validation before being successfully uploaded into SEVPAMS.

- Adjudication
- Compliance
- Investigative
- Communication and Customer Relations

**Category of Users with System Access:**[45]
- Federal Government Personnel

**Category of Individuals Impacted:**
- F and M Nonimmigrants
- Schools
- School Officials
- School Employees
- School Partner
- J Nonimmigrants
- Exchange Visitor Programs
- Program Officials
- Host Families
- Federal Government Personnel
- State Government Personnel
- Governing Bodies
- Members of the Public
- Employer Information

**Sources of Information:**
- Federal Government Personnel
- Federal Government Systems

**Category of Information in the System:**
- Biographical
- Identity Verification
- Education
- Program
- Employment
- Financial
- Travel
- Immigration-Related
- School
- Program Sponsor
- Case-Related
- Auditing and Training
- Reporting
- Inquiries and Data Corrections

[45] For information on system access controls and other system safeguards, please see Section 7, Principle of Security.

## System Modules:

***Request for Information Management (RFI) Module***

The RFI provides SEVP with an automated process for requesting documents from external stakeholders (e.g., F, M, and J nonimmigrants, school officials, and Exchange Visitor Program sponsors). SEVP requests documents when an external stakeholder seeks action (e.g., a correction request), and the SEVPAMS RFI module links those documents to specific cases and inquiry tracking tickets.

**Category of Transactions:**

- Adjudication
- Compliance

**Category of Users with Access:**

- Federal Government Personnel

**Category of Individuals Impacted:**

- F and M Nonimmigrants
- School Officials

**Sources of Information:**

- F and M Nonimmigrants
- School Officials

**Category of Information:**

- Biographical
- Identity Verification
- School
- Employment
- Immigration-Related
- Case-Related

***SEVPAMS Inquiry Tracking Tool – Customer Relationship Management (CRM)***

The CRM allows SEVP personnel to track inquiries received by SEVP (e.g., email, telephone calls related to general questions, data correction requests, and technical issues identified by external requesters including Federal Government personnel, school and program officials, and F/M/J nonimmigrants).[46] Specific information collected from the requester is determined by the nature of the inquiry. For example, students may inquire about how to maintain status or pay required fees. School officials may inquire about changing a student's status, request data maintained by SEVP be corrected, or request information on their school or school official recertification status. The public may inquire about SEVP regulations. SEVIS users might contact SEVP about technical issues such as password resets or other SEVIS access issues. SEVP personnel manually review SEVIS information to validate the individual's identity for inquiries and technical issues related to that individual or school and program (i.e., data fixes to update information in SEVIS). This information is used to ensure data integrity and delivery of proper instructions and guidance to the customer.

**Category of Transactions:**

- Communication and Customer Relations

**Category of Users with Access:**

- Federal Government Personnel

**Category of Individuals Impacted:**

- F and M Nonimmigrants
- J Nonimmigrants
- Program Officials
- Exchange Visitor Programs
- Host Families
- Schools
- School Officials
- School Employees
- School Partner
- Federal Government Personnel
- State Government Personnel
- Governing Bodies
- Members of the Public

**Sources of Information:**

- Federal Government Personnel
- Federal Government System

**Category of Information:**

- Biographical
- Identity Verification
- Administrative
- Employment
- Financial
- Travel
- Immigration-Related
- School
- Case-Related
- Auditing
- Reporting
- Inquiries and Data Corrections

[46] On occasion, individuals from the public, members of Congress and their staff, as well as attorneys for F/M/J nonimmigrants and schools or exchange visitor programs, may reach out to SEVP with inquiries.

***SEVP Analysis and Operations Center (SAOC) Tip Log***

The SAOC tip log allows SEVP to track, review, and investigate tips received from members of the public, F/M/J nonimmigrants, and school officials. These tips are related to potentially noncompliant activities by schools, programs and their officials, and F/M/J nonimmigrants. Tips are reviewed to determine their validity and to identify the next action to take regarding potential noncompliance activity.[47]

**Category of Transactions:**

- Compliance
- Investigative

**Category of Users with Access:**

- Federal Government Personnel

**Category of Individuals Impacted:**

- F and M Nonimmigrants
- J Nonimmigrants
- Program Officials
- Exchange Visitor Programs
- Host Families
- Schools
- School Officials
- Federal Government Personnel

**Sources of Information:**

- Federal Government Personnel
- Members of the Public
- F and M Nonimmigrants
- J Nonimmigrants
- School Officials
- Program Officials

**Categories of Information:**

- Biographical
- Immigration-Related
- Employment
- Case-Related

[47] Before any adverse action is taken by ICE, SEVP SAOC coordinates with other ICE law enforcement offices/units (e.g., CTCEU) to investigate the tip.