Privacy Impact Assessment Update
for the

Student and Exchange Visitor Information System (SEVIS); Student and Exchange Visitor Program Automated Management System (SEVPAMS); and SEVP External Training Application (SETA)

DHS/ICE/PIA-001(c)

June 15, 2017

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) is a program within the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) that owns and operates: 1) the Student and Exchange Visitor Information System (SEVIS) and 2) the Student and Exchange Visitor Program Automated Management System (SEVPAMS). SEVIS is an Internet-based system that maintains real-time information on nonimmigrant students and exchange visitors, their dependents, and schools and sponsors that host these nonimmigrants. The original Privacy Impact Assessment (PIA) for SEVIS was published on February 5, 2005 (2005 SEVIS PIA) and updated on July 19, 2016. This update provides notice of: 1) new or updated SEVIS sub-systems: (SEVP Portal and SEVIS Professional I-515A Tracking System (SPITS)); 2) new SEVP External Training Application (SETA); and 3) new SEVPAMS functionality.

Overview

U.S. Immigration and Customs Enforcement (ICE) operates the Student and Exchange Visitor Program (SEVP) under the authority of 8 U.S.C. § 1372, and is required to develop and manage a program to electronically collect, from approved educational institutions and designated exchange visitor programs in the United States, certain information about aliens who have or are applying for F, M, or J nonimmigrant (hereafter "F/M/J nonimmigrant") status.[1] Section 1372 also requires that particular information be collected, such as identifying information about the alien; field of study, status, and compliance information from educational institutions and exchange visitor programs; and the alien's date and port of entry. SEVP coordinates with the U.S. Department of State (DoS), which oversees the operation of the exchange visitor program including the designation of exchange visitor programs.[2] As discussed below, SEVP operates the Student and Exchange Visitor Information System (SEVIS) and oversees the student program including the certification of schools. The following provides an overview of the new or updated

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

[2] Congress mandated that DHS (originally the Department of Justice), in consultation with the U.S. Department of State (DoS) and the 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. DoS oversees exchange visitors (*i.e.*, nonimmigrants who enter the United States on J class of admission), and the exchange visitor programs (*e.g.*, 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.

SEVP systems.

Student and Exchange Visitor Information System (SEVIS)

SEVIS is an Internet-based system, located on-site at ICE, 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 and spouses (F-2, M-2, and J-2 classes of admission).[3] Designated school officials (hereafter "school officials") of SEVP-certified schools, and responsible officers (hereafter "program officials") of DoS-approved exchange visitor programs use SEVIS to transmit mandatory information and event notifications about F/M/J nonimmigrants via the Internet to DHS and DoS.[4] SEVIS manages and tracks information for participating F nonimmigrant students related to their practical training. SEVIS also monitors and tracks those F/M/J nonimmigrants who have gained entry into the United States through the Form I-515A, *Notice to Student or Exchange Visitor* (Form I-515A) process, a deferred inspection to ensure compliance with entry requirements.[5]

The following are new or updated SEVIS sub-systems or other systems associated with the SEVP program that will be discussed in more detail in this PIA update:

SEVP Portal

SEVP will launch the SEVP Portal, a new SEVIS sub-system that manages and keeps track of Optional Practical Training (OPT). OPT allows F nonimmigrant students studying in the United States an opportunity to gain practical work experience in their field of study. This new SEVP Portal secure web interface permits F 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).[6] The F nonimmigrant is also able to directly edit their OPT employment information, rather than relying on school officials to update this information on behalf of the F nonimmigrant student.

SEVIS Professional I-515A Tracking System (SPITS)

SPITS is an SEVP system that was established in 2010 as a Microsoft Access database, and with this PIA update, it will become a new SEVIS sub-system. SPITS is used by SEVP staff to analyze, adjudicate, track, and manage the activities and documents required from F/M/J nonimmigrants, including their dependents, as part of the Form I-515A instructions. When a F/M/J nonimmigrant lacks proper documentation at a Port of Entry to enter the United States (*e.g.*, forgot

[3] Hereafter, this PIA update will refer to nonimmigrant students, exchange visitors, their spouses, and dependents as F/M/J nonimmigrants collectively.
[4] A comprehensive description of SEVIS data elements is contained within the DHS/ICE/PIA-001 Student and Visitor Exchange Information System (SEVIS) (February 5, 2005), *available at* www.dhs.gov/privacy.
[5] The Form I-515A, *Notice to Student or Exchange Visitor* is *available at* https://www.ice.gov/doclib/news/library/forms/pdf/i515a.pdf.
[6] These changes may be made by school officials, with the appropriate documentation.

Form I-20 *Certificate of Eligibility for Nonimmigrant and Student Status*, out of status)[7], he or she is referred to secondary inspection where U.S. Customs and Border Protection (CBP) conducts vetting checks and issues a Form I-515A, if the nonimmigrant is deemed otherwise admissible into the United States. The Form I-515A allows the nonimmigrant temporary, lawful status, and 30 days to satisfy the requirements listed on the Form I-515A and to submit evidence to SEVP. SEVP must receive the original Form I-515A and required documents prior to expiration of the 30-day period. If the documentation is not received in time, SEVP terminates the F/M/J nonimmigrant's status in SEVIS. The nonimmigrant must then either leave the United States or apply to DHS's U.S. Citizenship and Immigration Services (USCIS) for reinstatement.

SEVP External Training Application (SETA)

SETA is a new learning management tool that provides training to SEVP stakeholders, including Federal Government officials, school and program officials, and F/M/J nonimmigrants.[8] SETA provides a single location to access 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, including OPT, for F nonimmigrant students.

Student and Exchange Visitor Program Automated Management System (SEVPAMS)

SEVPAMS is an existing SEVP system that provides automated workflow capabilities, collaboration workspace, document repository, and electronic records management for SEVP records.[9] Primarily, SEVP uses SEVPAMS to maintain documentation received from SEVP stakeholders to validate information entered into SEVIS, including F/M/J nonimmigrants, school officials, and Federal Government officials for identification and validation purposes related to such activities as school certification, Form I-515A compliance, and SEVP system access.

With this PIA update, SEVPAMS will provide several new functions. First, a new two-way interconnection between SEVIS and SEVPAMS (hereafter "SEVIS-SEVPAMS interconnection") will be established, which allows status and messaging related to SEVP activities to be exchanged. Second, SEVP will use new functionality in SEVPAMS to track and manage correction requests made by school officials who submit requests to correct F/M nonimmigrant data in SEVIS. Third, SEVP will use the SEVIS-SEVPAMS interconnection to track and manage Form I-17 *Petition for Approval of School for Attendance by Nonimmigrant Student*, (hereafter

[7] Form I-20 is used by SEVP for F-1 and M-1 nonimmigrants. Form I-20 is not publicly available, it is provided only by designated school officials or sponsors.
[8] On occasion, individuals from the public, such as members of Congress and attorneys for F/M/J nonimmigrants and schools or exchange visitor programs, may create a SETA account to access the training courses available in SETA.
[9] SEVP launched SEVPAMS in 2009, and ICE completed a Privacy Threshold Analysis (PTA) on SEVPAMS at that time. Based on the PTA, DHS determined an update to the SEVIS PIA was not required. SEVPAMS was also determined to be covered under the DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records Notice. In the interest of transparency, ICE is including SEVPAMS in this PIA update.

"Form I-17") information submitted by schools for initial certification, recertification, and update petitions, as well as appeals. Fourth, new functionality in SEVIS and SEVPAMS will allow school officials to use SEVIS, as a pass-through system, to upload documents into SEVPAMS,[10] allowing for more secure and efficient receipt by SEVP staff.

Lastly, this PIA update also describes new functionality in SEVPAMS that will be used to provide customer service to F/M/J nonimmigrants, school and program officials, Federal Government officials, and the public (*e.g.*, attorneys, members of Congress), by managing and tracking general inquiries and technical issues that are received by SEVP staff via phone and email. SEVPAMS will use SEVIS information to validate the identity of the individual for inquiries and technical issues that are specific to an individual or school and program (*e.g.*, data fixes to update information in SEVIS). This information is collected to ensure data integrity and proper instructions and guidance are delivered to the customer.

Reason for the PIA Update

DHS/ICE is updating the SEVIS PIA[11] to provide notice of: 1) new or updated SEVIS sub-systems (SEVP Portal and SEVIS Professional I-515A Tracking System (SPITS)); 2) the new SEVP External Training Application (SETA); and 3) new SEVPAMS functionality. Additionally, the new SEVIS sub-systems (SEVP Portal and SPITS), SETA, and SEVPAMS will now be located in secure Internet cloud environments.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

Legal Authorities

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, U.S.A. PATRIOT Act; Public Law 107-173, Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act); 8 CFR 214.2(f), (j), and (m); 8 CFR 214.3; 8 CFR 214.4; 8 CFR

[10] Documents uploaded via SEVIS are scanned for any viruses via a virus checker, and must pass the checks before the documents can be uploaded into SEVPAMS.

[11] *See supra* note 4.

214.5; 22 CFR Part 62; 8 CFR 214.12; 8 CFR 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).

System of Records Notice (SORN)

SEVIS and SEVPAMS data are covered under the existing DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) System of Records Notice (SORN).[12] SEVPAMS inquiry tracking is covered under the following existing DHS/ALL-016 DHS Correspondence Records SORN[13] and SETA is covered under the existing DHS/ALL-003 DHS General Training Records SORN.[14]

System Security Plans

Both SEVIS and SEVPAMS have a system security plan in place. The systems have completed a certification and accreditation (C&A) process that reviews security tools and procedures that are in place for each system. This C&A process also ensures that they are following established policies. A single C&A package is currently being completed to cover SEVP Portal, SPITS, and SETA.

SEVIS and SEVPAMS were separately granted a 36-month Authority to Operate (ATO) by ICE Office of the Chief Information Officer. The ATO process entailed a review of both SEVIS and SEVPAMS documentation and a Security Controls Assessment. The SEVIS ATO covers the current SEVIS; however, a new SEVIS Modernization ATO, currently under development and review, will cover the deployment of SEVP Portal, SPITS and SETA, and the use of a secure Internet cloud environment to manage these new SEVP systems. Separately, a new SEVPAMS ATO, currently under development and review, will replace the current SEVPAMS ATO and will cover the SEVPAMS migration into a secure Internet cloud environment.

Characterization of the Information

SEVP Portal

The primary purpose of the new SEVP Portal is to allow F nonimmigrant students to review, enter, and update their OPT employment information, and some of their biographical information via a secure web interface. F nonimmigrant students with OPT approval will be able to access the SEVP Portal in order to review their name, date of birth, gender, country of birth and citizenship, SEVIS ID (used to link the records between SEVIS and SEVP Portal, and used as a

[12] DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS), 75 FR 412, (Jan. 5, 2010).
[13] DHS/ALL-016 Department of Homeland Security Correspondence Records, 73 FR 66657 (Nov. 10, 2008).
[14] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (Nov. 25, 2008).

secondary authentication within SEVP Portal), and contact information such as address, email address, and telephone number. With the exception of the student's name, SEVIS ID, date of birth, gender, country of birth and citizenship, and his or her email address (used for logging into SEVP Portal), the nonimmigrant student will be able to modify the data mentioned above. This data are all pre-populated into SEVP Portal from SEVIS data, which is directly entered into SEVIS by the school officials. When a school official updates any information (*e.g.*, gender, date of birth, country of birth), that updated information is sent from SEVIS to the SEVP Portal. The OPT employment information, including employment start and end dates, employer contact information, employer identification number (EIN), and employer official (supervisor) contact information,[15] is the only set of data that is not typically pre-populated by SEVIS, unless the data is already entered into SEVIS by the school official. Instead, the employment information will now be entered into SEVP Portal directly by the F nonimmigrant student. This collection of information directly from F nonimmigrant OPT students helps to ensure its accuracy. For those F nonimmigrant students participating in an extension to OPT as part of their course of study, pursuant to a qualifying science, technology, engineering, or math (STEM) degree, although they will be able to review and update data as mentioned above, they will not be able to enter new employer information into SEVP Portal. STEM OPT students still require school officials to enter new employer information since a school official has to review the Form I-983, *Training Plan for Science, Technology, Engineering & Mathematics Optional Practical Training* prior to recommending STEM OPT employment or employer changes.[16] School officials may also update OPT information directly in SEVIS for those F nonimmigrant students with access to SEVP Portal, if the student is unable to access the SEVP Portal for any reason.

SPITS

With the new version of SPITS,[17] there is no change to the information collected. Even the process for populating information into SPITS has not changed. The main change is related to where the information is maintained. Instead of being maintained in a Microsoft Access database, the information is now maintained in a sub-system of SEVIS, which provides a more secure means to manage the information and allows for the system to email F/M/J nonimmigrants and school and program officials directly.[18]

The information maintained in SPITS includes biographical information such as name, date of birth, country of citizenship, contact information, including telephone number and U.S. address,

[15] SEVP has been collecting this information in SEVIS under the broad employment authorization category. In the interest of transparency, ICE is identifying the specific data collected related to OPT employment information.

[16] The school official reviews the Form I-983 *d*, and must enter the new employer information for STEM OPT students into SEVIS.

[17] SEVP has been using the previous version of SPITS, an internal SEVP system, since 2010. In the interest of transparency, ICE is now identifying the specific information used and systems connected to SPITS.

[18] This change also brings SPITS within the coverage of a system security plan and ATO for SEVIS, improving the security and monitoring of the data.

and SEVIS ID; and travel information, including arrival and departure dates and Admission number. This information is pulled from SEVIS, CBP's Arrival Departure Information System (ADIS)[19], and from ICE's Enforcement Information Database (EID),[20] which stores information captured by Form I-515A and maintained in CBP's Secured Integrated Government Mainframe Access (SIGMA).[21]

SETA

SETA, a new learning management tool, provides Federal Government officials, school and program officials, and F/M/J nonimmigrants authorization to use the training resources in SETA. These authorized user groups, mentioned above, provide their name and email address to create a SETA account. Once registered, these authorized users can access SETA and the SEVP training courses, including their training transcripts.

SEVIS-SEVPAMS Interconnection

With the new direct interconnection between SEVIS and SEVPAMS, no new data is collected but the processing of existing data will change. The SEVIS-SEVPAMS interconnection will allow for: (1) real-time status updates and transaction messages to be sent between the systems; (2) track and manage correction requests, including status updates, for data updates to SEVP systems, particularly SEVIS; (3) track and manage I-17 petition information submitted by schools for initial, recertification, and update petitions as well as appeals; and (4) school officials are able to upload documents through SEVIS (as a pass-through) that will transfer and store documents in SEVPAMS, thereby streamlining an existing manual process.

First, this new two-way interconnection permits data to flow back and forth between SEVIS and SEVPAMS, allowing for near real-time status updates and school information, exchanges of transactional messages, and permitting pre-population of SEVIS data in SEVPAMS. Status updates push information (*e.g.*, SEVIS ID, status code) between both SEVIS and SEVPAMS when activities occur within the system, when a request to expedite an event is made, or when SEVP staff updates the status of the activity they are performing in SEVPAMS. Transaction messages include information like receipt acknowledgement (*e.g.*, date/time of receipt) when SEVPAMS receives an uploaded document from a school official, for example, and sends a message acknowledging when the document was received.

Second, better tracking and management of correction requests will occur with the use of the SEVIS-SEVPAMS interconnection. Correction requests are received from school officials, through SEVIS, to modify data contained in SEVIS related to F and M nonimmigrants. These

[19] *See* DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS), *available at* www.dhs.gov/privacy.
[20] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID), *available at* www.dhs.gov/privacy.
[21] SIGMA is a sub-system of Automated Targeting System-Targeting Framework (ATS-TF) with its own user interface. For more information *see* DHS/CBP/PIA-006(b) Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.

requests are pushed from SEVIS to SEVPAMS, where SEVP staff process and adjudicate the requests. As part of the correction request process, the SEVIS ID associated with the individual whose data is being modified is provided so that the information modified is associated with the correct record to help ensure accuracy of the information held in both SEVIS and SEVPAMS.

The data identified in the correction request is limited to those data fields that may not be edited by school officials and require additional documentation for validation in order for the information to be modified. For example, if a school official made a mistake and fails to update the student's full-time registration information, the student's SEVIS record will be terminated. A school official can ask to have the student record put back to active status by requesting a correction and providing evidence of enrollment. This request is pushed into SEVPAMS where SEVP staff receives the request and begins the adjudication process, to determine whether to make the change in the system or not. As part of this adjudication process by SEVP, documents are requested to validate the full time registration, such as a certificate transcript. Documents related to correction requests will be uploaded through SEVIS, as a pass-through system, to be stored in SEVPAMS. This will replace the current process of emailing documents to SEVP for manual upload.

Third, the SEVIS-SEVPAMS interconnection allows for the tracking and management of I-17 school petitions (*i.e.*, school certification, recertification, updates, and appeals). The I-17 petition information (*e.g.*, school information, campus information, school official biographical, including contact information) is transferred from SEVIS to SEVPAMS, allowing SEVPAMS to track the workflows and status of the school petitions and petition appeals. SEVP staff adjudicates the I-17 data to determine the school's SEVP certification status. SEVP certification of a school authorizes that school to enroll F and/or M nonimmigrant students in their programs. By obtaining SEVP certification, the school makes a legally binding commitment to comply with certain federal laws, regulations, and DHS requirements.

Lastly, the SEVIS-SEVPAMS interconnection also allows school officials the new ability to upload documents through SEVIS as evidence to support school certification, recertification, and updates for I-17 petition requirements as well as correction requests. These documents pass-through to SEVPAMS. Documents such as evidence of U.S. Citizenship or Lawful Permanent Residency for the school's officials, state licensure or exemption, accreditation from U.S. Department of Education, and teacher qualifications are uploaded by school officials and are used for evidence for school certification, updates, and recertification adjudication. The method of receiving these documents by upload is a new means to collect this information directly from the schools; previously these records were emailed or mailed to SEVP. The information associated with the document uploads, known as metadata (*e.g.*, document type, document ID, document size, filename), is typical of any electronic document upload. SEVIS automatically captures the identity of the user who uploads the information, which includes the collection of biographical information (*e.g.*, school official's name) used to identify the person uploading the information; the associated organization (*e.g*., school name, school code) whose documents were uploaded; unique identifiers (*e.g*., SEVIS ID); and, activity tracking numbers (*e.g*., Petition ID, Correction Request ID) are used to validate accurate record matching and tracking purposes. This information also populates in SEVPAMS with the upload of the document. The type and volume of documents will not change, only the source of submission. All documents are scanned for viruses before they pass through from SEVIS to SEVPAMS to ensure the systems remain safe from a potential virus infection.

SEVPAMS Inquiry Tracking

With this PIA update, SEVPAMS will have the ability to track inquiries (*e.g*., email, telephone calls) received by the SEVP Response Center related to both general questions and technical issues identified by external requesters including federal government officials, school and program officials, F/M/J nonimmigrants, and the public (*e.g*., attorneys, members of Congress). Although this inquiry tracking functionality is new for SEVPAMS, the SEVP Response Center previously tracked these inquiries and collected information from requesters using another ICE tracking system managed by the ICE Office of the Chief Information Officer.

The information collected to track inquiries is not new, only where the data resides is new. SEVP Response Center staff input biographical information into SEVPAMS. At a minimum, name, telephone number, and email address is collected from requesters, which allows the SEVP Response Center staff to get back in touch with the requester if a call drops or to follow back up with the requester on his or her question or technical issue. For Federal Government officials, school and program officials, and F/M/J nonimmigrants, additional information is collected by the SEVP Response Center staff and entered into SEVPAMS for purposes of inquiry tracking. This information includes: biographical [*e.g*., name, truncated date of birth (only for F/M/J nonimmigrants) (*i.e*., day and month), contact information such as email address and telephone number, unique identifier (*e.g*., SEVIS ID, Requester ID for tracking inquiries)] information, identifying the government agency for a Federal Government official, and school/program information (*e.g*., school/program name, school/program code, field representative unit territory, location information). On occasion, school and program officials may also email documentation to SEVP related to their inquiry. For example, a school official will send an official letter asking SEVP to change a student's status from completed to active as the student will be participating in OPT. This documentation is uploaded manually into SEVPAMS by the SEVP Response Center staff. The specific information collected from the requester is determined by the nature of the inquiry. For example, F/M/J nonimmigrants may make inquiries about how to maintain their status, or pay their required fees; school officials have inquiries about changing a student's status if it was cancelled and needs to become active, recertification of their school or program officials about the re-designation of their exchange visitor program; the public may make inquires related to SEVP regulations; and SEVIS users might contact SEVP Response Center about technical issues, such as password resets or other issues related to SEVIS access.

Privacy Risk: There is a risk that the systems could contain inaccurate information.

Mitigation: This risk is partially mitigated in SEVP Portal, SETA, and SEVPAMS as more information in the systems is collected directly from the individuals who are the subject of the data, increasing the likelihood that the information is accurate.

This risk is partially mitigated in SEVP Portal and SPITS as the systems are configured so that when information is changed or updated in SEVIS, the data will then update in the other system and vice versa. This helps to eliminate the risk of stale or inaccurate data.

This risk is partially mitigated in SEVIS, SEVP Portal, SPITS, and SEVPAMS as individuals may request access to and correct their information in the system, if it is inaccurate. Although F/M/J nonimmigrants may not be given the privacy protections of the Privacy Act of 1974, 5 U.S.C. § 552a, SEVP does allow for correction of an individual's information in SEVP systems, which leads to improved data accuracy for systems. This can be done through a request to SEVP Response Center by the F/M/J nonimmigrant's school or program official through SEVIS, or by the F nonimmigrant OPT student through SEVP Portal. Additional documents to validate the data may be requested by SEVP, which helps to reduce the risk of having inaccurate or fraudulent data in the SEVP systems.

This risk is partially mitigated in SEVP Portal, SPITS, and SEVPAMS, through the use of pre-populated data from SEVIS and obtaining other data directly from other DHS systems, such as EID data for SPITS. The data is updated in real-time so that users are working with the most up-to-date data.

This risk is also partially mitigated in SEVIS because F and M nonimmigrant students are instructed to review their records, such as their travel and admission forms (*e.g.*, Form I-20, visa, and Form I-94), when they are issued for accuracy. Correcting mistakes early in the SEVP process is quicker and cheaper, and prevents confusion. By accepting the conditions of their class of admission from the U.S. government, nonimmigrant students have made a legal commitment and will need accurate records to verify their compliance.

Privacy Risk: There is a risk that the systems collect more information than is necessary for the purposes of the program.

Mitigation: This risk is partially mitigated by the use of structured pre-determined data fields that are necessary to fulfill the purpose of the collection. Drop-down lists and rule-based fields can limit what specific information can be added to the SEVP systems. Free text fields are also occasionally used, which causes a risk of collection of data beyond what is necessary. This risk is minimized by limiting the number of free text fields made available to system users. The majority of system data is captured in structured data fields, not free text fields, allowing for more consistent information maintained in the systems. Additionally, training and instructions are provided to the individuals, which are typically the school and program officials, entering information into the systems. These materials clearly identify what specific information should be entered into the specific field.

In addition to the use of structured data fields, there is also a formal process that requires ICE Office of Information Governance and Privacy and ICE Forms approval prior to collection of information from the public. All new and modified information collections from the public must be approved by ICE, including ICE Office of Information Governance and Privacy, and the Office of Principal Legal Advisor, prior to collection. ICE Office of Information Governance and Privacy reviews the information identified to be collected and determines whether the collection is acceptable, if the collection is compatible with the purpose of the collection, and whether the information collected is relevant and necessary to fulfill the purpose of the collection. ICE Office of Information Governance and Privacy also confirms with the Office of Principal Legal Advisor that ICE has the legal authority to collect the information prior to the form being approved. Data collected from F/M/J nonimmigrants, school and program officials, and Federal Government officials have been reviewed and approved as part of this formal process. Any additions or modifications to the data collection are reviewed and must be approved prior to collection.

Privacy Risk: SEVP systems are not configured to handle two-factor authentication (*e.g.*, password plus a token or smart ID card) for access by non-government users, which presents an increased risk of identity theft if information is compromised.

Mitigation: This risk is partially mitigated through the use of network controls, access controls, security monitoring, audits, and other authenticating tools to verify an individual. Federal Government officials are mandated to use two-factor authentication to access their respective networks. It is the policy of DHS that its employees, including contractors, use the DHS network to access DHS information, especially when accessing or handling information that is Sensitive personally identifiable information (PII).[22] Requiring DHS employees to work within a secured network environment adds a layer of protection when accessing the information in SEVP systems, even if those systems are not currently configured with two-factor authentication at this time. The use of two-factor authentication for all users of SEVP systems is being considered for future deployment. Two-factor authentication to access SEVP systems will provide even more secure access and help mitigate access by unauthorized users.

System administrators use access controls to ensure that only authorized users can access the data in the systems. Requiring user IDs and passwords limit the ability of unauthorized outsiders to access the systems. As identified in SEVP system training manuals, it is best practice to protect passwords and SEVIS users are warned that they must not share SEVIS passwords, as

[22] DHS defines Sensitive PII as “personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.” *Handbook for Safeguarding Sensitive Personally Identifiable Information* (March 2012) https://www.dhs.gov/publication/dhs-handbook-safeguarding-sensitive-pii.

it is a violation of DHS Sensitive Systems Policy Directive 4300A (March 14, 2011) and will result in disciplinary action. Passwords are also required to be changed every 90 days. There are specific length and limitations as to creating a password for SEVP systems.

In addition to user ID and passwords, access roles are used for managing what information is made available to what individuals. Access roles are designated by the category of individual (*e.g.*, Federal Government officials) and by the individual's position, which helps ensure that access is granted only to those with a need to know information in order to perform their official duties. Not only do access roles limit access to specific types of information, access roles can also limit access so that certain user groups may only have "read only" access to specific information types they are allowed to access, while other groups have read/write/edit privileges again based on the system user's roles and responsibilities.

Individuals cannot access the systems without an account created by the system's administrator. Only system administrators can make changes to the system and grant access to other authorized users. System administrator accounts are immutable, meaning the accounts are assigned to specific individuals. These accounts are audited, monitored, and reviewed the same as all other system user accounts. Audit reports are reviewed by SEVP, ICE, and DHS, which allows for multiple levels to review and identify misuse of system access, even by system administrators.

The SEVIS Accounts Management Team removes SEVIS access for users who no longer require access to the system. The SEVIS Accounts Management Team has the authority to add and remove SEVIS access upon request from federal or contract managers. Schools and program officials also have system privileges to remove access for users who no longer work for them or no longer need access to SEVIS. If individuals with SEVIS access do not access SEVIS for 45 days, their access is automatically disabled and they are required to re-initiate the system access process. Additionally, every year all SEVIS users must have their continued need for access in their assigned role validated.[23] Federal supervisors validate government users. For schools, the school official validates continued user access. For programs, the program official validates continued user access.[24] If user access is no longer needed, the SEVIS Accounts Management Team removes the user's access privileges. At this time, the SEVIS Accounts Management Team does not perform any additional periodic review of user accounts.

Information System Security Officers (ISSO) perform routine reviews to monitor security and check for misuse by authorized users, including system administrators, or for evidence of unauthorized intrusion into the systems *i.e.*, hacking. ISSOs actively review user activities for unauthorized actions including the unauthorized removal of data and the modification or

[23] This user account review process is in compliance with *DHS 4300A Sensitive Systems Handbook*, https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook and the *Federal Information Security Management Act (FISMA)*, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

[24] PDSO/DSO Annual Verification, *available at* https://studyinthestates.dhs.gov/sevis-help-hub/update-records/manage-school-records/school-certification/form-i-17-petition-update/pdsodso-annual-verification.

disablement of security controls. ISSOs review activities such as successful logins, failed logins, failed authentications, and review a summary of accesses regularly. SEVIS users are provided notice before accessing the system, during SEVIS training, that their use is monitored.

In addition to information collected directly via SEVP systems, SEVP also receives Sensitive PII from school officials via email. SEVP guidance recommends that school officials zip and encrypt documents emailed to SEVP for school certification. This activity will be replaced with the use of SEVIS-SEVPAMS interconnection by uploading documents to SEVIS, as a pass-through to maintain in SEVPAMS.

Privacy Risk: For SEVP Portal, there is a risk that F nonimmigrant OPT students will enter fraudulent or incorrect information into the system.

Mitigation: Although collecting information directly from an individual to whom it pertains is usually the best method for ensuring data quality, the risk that an individual will provide fraudulent or incorrect information still remains.

Prior to the deployment of SEVP Portal, F nonimmigrant students with OPT were required to provide the employment information, and any updated information such as their address, to the school official, who would enter the information into SEVIS. The school official would review his or her documentation to verify that the information provided by the student was legitimate. There is an incentive for school officials to provide accurate information into SEVIS. 8 CFR 2143 (a)(1)(ii) states that if school officials provide willful misstatements, that may constitute perjury (18 U.S.C. 1621), which could result in fines and/or imprisonment. With the launch of the SEVP Portal, the F nonimmigrant student with OPT can now directly review, enter, and update his or her own personal and employment information.

There continues to be a risk that fraudulent or innocently entered incorrect information may be added, even though school officials retain the ability to review and verify information. One form of mitigation used to limit fraudulent entered into SEVP Portal occurs just after the F nonimmigrant logs into SEVP Portal, but prior to any access to the system data. The F nonimmigrant student must accept the following attestation before entering the SEVP Portal to view, enter, and modify his or her information.

> When using the SEVP Portal, providing materially false, fictitious, or fraudulent information may subject you to criminal prosecution under 18 U.S.C. 1001. Providing willful misstatements may constitute perjury under 18 U.S.C. 1621. Other possible criminal and civil violations may also apply.

School officials should still review the information provided, but they may not have the means to verify its accuracy. The school officials should also continue to request documentation to verify employment and even a change in mailing address. However, since the F nonimmigrant OPT student’s information is being pushed directly into SEVIS, school officials might not be as vigilant in reviewing the accuracy of the information provided by these students. This risk cannot be fully mitigated.

There are, however, some automated functions in SEVP Portal that may partially mitigate fraudulent or incorrect information from getting pushed through into SEVIS. For example, when the F nonimmigrant student updates the U.S. address for him or herself or for his or her employer, this information is validated against U.S. Postal Service (USPS) address records. If the information entered into the address field is not validated against USPS addresses, an error message will appear and the information will not be updated. Only valid addresses are accepted into the system.

Uses of the Information

SEVP Portal

The F nonimmigrant OPT students use SEVP Portal to review, update, or modify their biographical, contact, and employment information. SEVIS pre-populates the biographical and contact information into SEVP Portal. Employment information may also be pre-populated if previously entered into SEVIS by the school official; otherwise this information is entered into SEVP Portal by F nonimmigrant students. Any changes or additions to information made by the F nonimmigrant student are returned to and updated in SEVIS. This information is used to evaluate the F nonimmigrant students' compliance with OPT requirements, which helps ensure they maintain their lawful status while in the United States. The F nonimmigrant students' biographical, contact and employment information is tracked, by school officials, throughout the OPT period using SEVIS and SEVIS Portal.

SPITS

The information collected and maintained in SPITS allows SEVP to monitor F/M/J nonimmigrant's compliance with Form I-515A instructions, to perform deferred inspection to ensure compliance with entry requirements, to make appropriate updates in the relevant systems, and to determine if further investigation is needed. The use and purpose of the information collected has not changed from the previous version of SPITS.

The process to populate information into SPITS from SEVIS and other DHS systems has also remained the same. The process for populating SPITS with information from other DHS systems occurs as follows: If an F/M/J nonimmigrant is admitted into the United States, CBP enters the F/M/J nonimmigrant information into CBP's Secured Integrated Government Mainframe Access (SIGMA), a system CBP uses at U.S. ports of entry to process secondary adverse actions and benefits, and to create the completed Form I-515A. SIGMA then stores this information in ICE's EID. SPITS pulls the I-515A data to from EID into SPITS. In order to verify F/M/J nonimmigrants are in compliance with the Form I-515A instructions, SPITS confirms the data with CBP's ADIS for up-to-date departure information to confirm the individual has left the country if he/she was unable to satisfy the requirements listed on the Form I-515A instructions within 30 days of receipt of the Form I-515A.

SETA

The system is used by internal and external stakeholders including Federal Government officials, school and program officials, and F/M/J nonimmigrants for training and requires minimal biographical information (*i.e*., name and email) to create an account to access the system. SETA now permits SEVP to use this new collection of information to not only provide access to the system, and training courses, but to also track the training courses accessed, and the individual's progress in each course.

SEVIS-SEVPAMS Interconnection

The information collected and maintained in SEVPAMS as a result of the SEVIS-SEVPAMS interconnection is not new, nor is it a new use of the information. Rather, this change creates a new method of providing the information to SEVP and exchanging the information between SEVIS and SEVPAMS in an automated fashion.

SEVPAMS Inquiry Tracking

The information collected and maintained in SEVPAMS related to inquiry tracking is not a new collection, as it was previously collected by SEVP through another ICE system. The use of the information for data integrity and proper guidance delivery also remains the same. Instead, inquiry tracking activity is moved to a new location, within SEVPAMS, and continues to be handled by the same SEVP staff.

Privacy Risk: There is a risk that communications sent by SEVP to school officials, F/M/J nonimmigrants, and Federal Government officials outside of DHS may contain Sensitive PII and are not protected sufficiently during transit.

Mitigation: This risk is partially mitigated by reducing the amount of Sensitive PII sent in communication to school officials, F/M/J nonimmigrants, and Federal Government officials outside of DHS. However, typically the name and SEVIS ID for the individual is included in communications sent from SEVP to ensure the information within the message allows for the identification of the correct person. Context of the information in the message can also be considered Sensitive PII and will require appropriate steps to securely communicate the information to parties outside of DHS.

If communication to parties outside of DHS is sent by email, SEVP is required to encrypt Sensitive PII attached to such emails, according to DHS policy. Otherwise, SEVP communication is mailed via USPS First Class Mail to individuals, such as Termination Notices to F/M/J nonimmigrants related to SPITS and the I-515A process. Like email, SEVP follows the procedures for mailing per DHS policy.

SEVP plans to develop secure communication portals that will help to mitigate this risk and minimize distribution of Sensitive PII via email. An email would still be sent to a SEVIS user such as a school official, but rather than containing Sensitive PII, the email provides notice of a new message and link to the new message that resides on a SEVP system. The SEVIS user would then be required to click on the link, and then enter his or her login information for the SEVP system in order to access the message. Access to the message would not be through internal systems, such as SPITS, but instead through external-facing systems, such as SEVIS for school and program officials and SEVP Portal for F/M/J nonimmigrants.

<u>Privacy Risk</u>: There is a risk that individuals will use the information in the systems for purposes beyond what is described in this PIA.

<u>Mitigation</u>: This risk is partially mitigated by using a warning when SEVIS users are accessing reports. 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.

This risk is partially mitigated for Federal Government officials accessing SEVIS. They are required to sign a Rules of Behavior prior to accessing SEVIS, confirming that they will protect sensitive information from disclosure to unauthorized persons or groups. However, for school and program officials accessing SEVIS, similar declarations are not obtained. To partially mitigate this risk, ICE is developing Rules of Behavior for all users of SEVP systems, so that there is consistent protection and handling of sensitive information that is contained in the systems. These Rules of Behavior will need to be signed prior to initial access to SEVIS and other SEVP systems, as well as periodically when renewal of access occurs. Additional attestations, similar to above, will be developed for school and program officials, and Federal Government officials to accept after logging into SEVP systems and prior to their exposure to PII. This attestation could be similar to what is used in SEVP Portal, with an additional requirement about protecting the PII maintained within the system.

This risk of using information beyond its purpose will also be partially mitigated through education. ICE Office of Information Governance and Privacy is developing training to educate school and program officials, and eventually F/M/J nonimmigrants on the access, use, handling, and disclosure of information in SEVIS and SEVP Portal. This training will be mandatory for initial access to SEVIS and SEVP Portal and for periodic access renewal. SEVIS and other system training will emphasize the Rules of Behavior as well.

Notice

For SEVP Portal, SPITS, SETA, and SEVIS and SEVPAMS updates, notice about these changes are provided by this PIA update. General notice about the information maintained in the systems and how it is shared is provided by the DHS/ICE/PIA-001 SEVIS PIA (February 5, 2005),[25] the DHS/ICE/PIA-001(b) SEVIS Admissibility Indicator (SEVIS-AI) PIA Update (July 19, 2016),[26] and this PIA Update.

For SEVIS, SEVP Portal, SPITS, and SEVPAMS, information about the individuals whose information is maintained in the system, the information stored in the system, and how the information is used, can be found in the DHS/ICE-001 SEVIS SORN. Similarly, for the inquiry tracking function within SEVPAMS, this information can be found in the DHS/ALL-016 DHS Correspondence Records SORN[27] and for SETA in the DHS/ALL-003 DHS General Training Records SORN.[28] These SORNs also provide notice about how information in these systems may be shared, accessed, and corrected.

Privacy Risk: There is a risk that individuals may not be aware that their information may be contained within the system.

Mitigation: This risk is partially mitigated through the publication of the 2005 SEVIS PIA, the SEVIS-AI PIA Update, this PIA Update, and the corresponding SORNs.

This risk is partially mitigated by the fact that some information is collected directly from the individual, thereby making that person aware of the specific purpose for the collection. Notices, in the form of privacy statements, about the collection are made available to the individual at the time of collection, which identifies the purpose of the collection. This is true for school and program officials as they provide information on themselves and their school or program via SEVIS, including uploading required documents. The privacy statement language is appropriate for nonimmigrants and U.S. Citizens and Lawful Permanent Residents.[29] For information collected and maintained in SEVPAMS related to general inquiries and technical issues, this information is typically received by SEVP Response Center via telephone call. As it is not possible to provide

[25] *See* DHS/ICE/PIA-001 Student and Visitor Exchange Information System (SEVIS) (February 5, 2005), *available at* www.dhs.gov/privacy.
[26] *See* DHS/ICE/PIA-001(b) SEVIS Admissibility Indicator (SEVIS-AI) PIA (July 19, 2016), *available at* www.dhs.gov/privacy.
[27] DHS/ALL-016 Department of Homeland Security Correspondence Records, 73 FR 66657 (Nov. 10, 2008).
[28] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (Nov. 25, 2008).
[29] Privacy language was developed according to the DHS Memo 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.

written notice for telephone calls, a verbal notice is provided to inform individuals that they will need to provide personal information to help resolve their inquiries and technical issues.

Data Retention by the project

There is no change to the retention of SEVIS data. The SEVIS records schedule will apply, which requires retention of the data for 75 years. This covers SEVIS information in the new SEVIS sub-systems.

SEVPAMS data will be retained according to the retention periods laid out in the National Archives and Records Administration (NARA)-approved general records schedules (GRS). The GRS can be found at http://www.archives.gov/records-mgmt/grs.html. GRS schedules cover the retention period of records that most agencies create and manage, for example system access forms. The majority of SEVPAMS records fall under a two year retention period. Much of the documentation contained in SEVPAMS are drafts or copies of final documents. The official final record tends to be owned by another office or agency, therefore the retention period can be quite short. However, there are instances when a more specific retention schedule will be needed to determine for specific SEVPAMS records. For example, the retention of SEVP case files maintained in SEVPAMS on activities such as school certification is currently under discussion. The possible retention for these case files range from 75 years, as the information is directly tied to the information managed in SEVIS, to a proposed retention for two school recertification cycles plus four years resulting in a ten-year retention. In this instance, discussion is needed to determine which period of time is most appropriate before a specific retention schedule is determined and approved.

Privacy Risk: There is a risk that information in SEVIS and SEVPAMS is retained longer than necessary to accomplish the purpose for which it was originally collected.

Mitigation: This risk is minimized for SEVIS and its sub-systems as the retention period is consistent with the existing retention schedule. The retention period is reviewed and discussed by ICE’s Privacy and Records Management offices, as well as the Office of the Principal Legal Advisor in conjunction with SEVP and the NARA archivist who works with ICE. The retention period is based on the administrative, fiscal, and legal value of the records, as well as privacy considerations. Consensus on the retention period must be reached prior to submission to NARA. Similarly, the risk for SEVPAMS is partially mitigated using the GRS and shorter retention periods. Managing how reference documents and copies of final documents can be made available while limiting over retention and duplication will continue to be reviewed and reduced as possible.

Privacy Risk: There is a risk that SEVIS information will not be properly disposed of or deleted at the end of the retention period.

<u>Mitigation</u>: This risk is partially mitigated by the fact that SEVIS records are scheduled for 75 years, so at this time no SEVIS records have been destroyed. However, for SEVPAMS, SEVP has a records management tool in place to manage and dispose of records according to the GRS. This tool is Department of Defense Directive 5015.2 (also known as DoD 5015.2)-compliant, a standard used to manage electronic records and that complies with NARA guidance. ICE officers and employees provide certificates of destruction (or other applicable documentation) to the ICE Office of Information Governance and Privacy, Records Division indicating that the records in the system have been appropriately disposed.

Information Sharing

External sharing and disclosure of SEVIS data does not change with this update. Internal sharing of SEVIS data will change in terms of the method of sharing and what is shared. Much of the changed internal information sharing is simply a switch from a manual internal sharing process to one that is now automated. For example, schools currently provide various documents to supplement their certification and recertification package by mail or email. With the new SEVIS-SEVPAMS interconnection, schools will be able to upload these documents directly into SEVIS, where they are automatically saved within SEVPAMS. SEVIS and SEVPAMS exchange messages of transaction statuses (*e.g.*, information received, time/date received and updated, document uploaded and received), which is used to verify the automated upload from SEVIS to SEVPAMS.

Also, the new information sharing established between SEVIS and the new SEVIS sub-systems now pre-populates SEVIS data in the new SEVIS sub-systems, which enhances the accuracy and timeliness of information.

<u>Privacy Risk</u>: There is a risk that the use of automated transfer of data between these systems will result in poor data quality.

<u>Mitigation</u>: This risk is partially mitigated by direct user input, which helps to ensure the accuracy of the data provided by school and program officials on their own school or program and their students or exchange visitors. For SEVP Portal, the information is directly collected from the F nonimmigrant OPT student. Accurate data helps facilitate correct connections between records when automating data transfers.

Data consistency also helps ensure data quality. Data exchanged between SEVP systems requires specific data, such as name, date of birth, email address, SEVIS ID, to ensure the data being pre-populated or exchanged automatically matches with the record maintained in the systems. To help facilitate matching between systems, consistent use of fields and information is used. When information is entered into SEVP systems, such as SEVIS, the majority of data is entered through the selection of dropdown options, rather than free text fields, which may often result in misspellings or other errors. Free text fields are still used for some data collection, but are limited in number and by who can enter data into those fields. For SEVIS, the individual entering the data in a free text field is typically the school or program officials.

Further information consistency is ensured by using business rules. Some of the data fields require the data be entered in a specific format that can also help to automatically identify errors in the information. For example, the date field can cause matching issues when the format of the date is entered in different ways (*e.g.*, the U.S. standard for dates is month, day, and year, while most other countries use day, month, and year). Additionally, if a date of birth was entered that identifies an individual outside an established acceptable range, such as identifying a person as being 180 years old, or a student as being three years old, the business rules in the field would identify this information as being an error. Only when the information is entered in the appropriate format and within the available range established by the business rule, would the information be accepted by the system.

Redress

The right to request amendment of records under the Privacy Act of 1974 (5 U.S.C. §552a) (Privacy Act) is limited to United States citizens and lawful permanent residents. Executive Order No. 13468, *Enhancing Public Safety in the Interior of the United States (EO 13,768)*, (January 25, 2017), which states: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information," precludes DHS from extending such rights by policy. The Judicial Redress Act of 2015 (Judicial Redress Act) (5 U.S.C. §552a note), 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.[30]

As a result of EO 13,768, DHS's "Mixed Systems Policy"[31] was cancelled by the DHS Privacy Office in its EO 13,768 implementing guidance.[32] This changes the ability of F/M/J

[30] The foreign countries and regional organizations covered by the Judicial Redress Act, 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 Judicial Redress Act, please visit the U.S. Department of Justice website https://www.justice.gov/opcl/judicial-redress-act-2015.

[31] The DHS's "Mixed Systems Policy" extended most Privacy Act protections to visitors and aliens whose information was collected, used, maintained, or disseminated in connection with a mixed system of records (*i.e.*, contains PII on U.S. citizens and lawful permanent residents, and non-U.S. citizens and non-legal permanent residents). Memorandum Number 2007-1, *DHS Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[32] DHS Memorandum 2017-01: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of 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, Executive Order 13768, does not affect statutory or regulatory privacy protections that may be afforded to aliens, such as confidentiality rights for asylees and refugees, and individuals protected under 8 U.S.C. §1367. These

nonimmigrants to access and correct their records maintained in a system of records at DHS, such as SEVIS or other SEVP systems. Individuals not covered by the Privacy Act or the Judicial Redress Act may access their records by filing a Freedom of Information Act (FOIA) request. In addition, the DHS implementing guidance makes clear that DHS 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 serves to undermine efficient decision making by DHS personnel, and can create the risk of errors made by DHS and its personnel. Also, PIAs are published, in part, to ensure that projects, programs, and systems maintain accurate data.

SEVP has an independent operational need to ensure that F/M/J nonimmigrant data is accurate, relevant, timely, and complete. An F/M/J nonimmigrant may correct his or her information maintained by SEVP in a few ways. First, the F/M/J nonimmigrant may contact his or her school or program official to have his or her official update the information in SEVIS. Second, the F/M/J nonimmigrant may contact the SEVIS Response Center to make a request to update his or her data in SEVP systems. Third, F nonimmigrant OPT students with SEVP Portal access may update specific information about themselves and their employer in the SEVP Portal.

Auditing and Accountability

Training

Step-by-step instructions and demos are provided to school and program officials accessing SEVIS and who enter F/M/J information into SEVIS. These instructions and demos are available via www.StudyintheStates.dhs.gov. Additional instructions and demos will be developed and made available related to the use of SEVP Portal and SETA. Internal instructions will be developed and made available to SEVP staff that will use SPITS and the SEVPAMS inquiry tool.

In addition, a new privacy and security training is under development and will fill a gap for providing knowledge and outlining consequences for misuse of the information in SEVP systems. This training will be made available through SETA. Possible consequences related to the misuse of information by school and program officials could be the removal of the official's access to the SEVP system, or even removal of the school's SEVP-accreditation or exchange visitor program's DoS-designation, thereby removing the ability for F/M/J nonimmigrants to continue to attend their school or program.

laws operate independently of the Privacy Act to restrict federal agencies' ability to share certain information about visitors and aliens, regardless of a person's immigration status.

Auditing

Security auditing is a shared responsibility between DHS, the ICE Chief Information Security Officer (CISO), and ISSOs. All are responsible for coordinating, implementing, and managing technology security regulations and requirements, which includes actively reviewing system security logs to identify threats to the systems.

SEVP systems, including SEVIS, SEVP Portal, SPITS, SETA, and SEVPAMS, maintain audit logs of user activity, including system administrator accounts, to monitor unusual behavior in the system. Audit logs track when individuals are logged into the system, who views which records, and how records are used within the system. Audit records are detailed enough to allow for the reconstruction of events if the system is compromised or a system malfunction occurs. At a minimum, audit records identify all unauthorized creation, changes, or removal of accounts, system configurations and database information. Audit logs are also used to track information shared with external parties. This allows ICE to track disclosures and ensure that information is being shared consistent with the provisions of this PIA and applicable SORN.

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 internal affairs office for investigation. The federal employee will be disciplined according to his or her agency policy, which could include adverse actions or removal from federal service. For non-federal 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. ISSOs routinely monitor misuse of the systems, and may revoke access to SEVIS for those who abuse their privileges; violations may also be reported to the proper law enforcement. If there are unexplained system events that raise suspicion for possible further investigation, then the ICE CISO is notified.

SEVP system audit logs are reviewed and reported on a regular basis by the ISSO to detect unusual activity within the system (*e.g.*, login times, number of logins attempts, failed login attempts, changes to records). This ensures that the system is being used appropriately. The ISSO audit reports are the basis for incident investigations and determinations. Further protection of information contained in the systems is enhanced through education. DHS staff is required to complete annual mandatory DHS privacy and information security training. Both trainings identify how to best protect the information collected and maintained by DHS. Required privacy and information security training will also be accessed through SETA by SEVIS users.

Cloud Computing

With this PIA Update, the new SEVIS sub-systems (SEVP Portal and SPITS), SETA, and SEVPAMS will be located in secure Internet cloud environments. All ICE records maintained in these systems will be located in the United States. Just like any other new location, appropriate security and privacy controls are in place and reviewed. An authority to operate (ATO) is required and will be completed prior to system deployment. SEVIS (except for SEVP Portal and SPITS sub-systems) will not be moved to an Internet cloud environment at this time.

Responsible Official

Lyn Rahilly
Assistant Director for Information Governance and Privacy
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

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