Privacy Impact Assessment
for the

ICE Use of Facial Recognition Services

DHS/ICE/PIA-054

May 13, 2020

Contact Point
Alysa D. Erichs
Acting Executive Associate Director, Homeland Security Investigations
U.S. Immigration & Customs Enforcement
Department of Homeland Security
(202) 732-5100

Reviewing Official
Dena Kozanas
Chief Privacy Officer Department of Homeland Security
(202) 343-1717

Abstract

Homeland Security Investigations (HSI) is the investigative arm of U.S. Immigration and Customs Enforcement (ICE) and is focused on countering domestic and transnational crimes. In the course of its investigations, HSI routinely encounters digital images of potential victims or individuals suspected of crimes but cannot connect those images to identifiable information through existing investigative means and methods. HSI, therefore, submits those images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes. The agencies and vendors query their databases for potential matches and return lists of potential candidate matches that HSI can use to produce investigative leads. HSI is conducting this Privacy Impact Assessment (PIA) because the use of these facial recognition services (FRS) requires the collection, maintenance, and use of personally identifiable information (PII).

Introduction

Facial Recognition Technology

Developments in machine learning, artificial intelligence (AI), and cloud technologies have drastically increased the speed and efficiency at which large volumes of data can be processed. These developments have enabled advances in face-based biometric identification called facial recognition. Facial recognition technology uses an AI algorithm to analyze human faces captured in photo or video footage. The facial recognition AI identifies facial landmarks such as eyes, bone structure, lips, nose, and mouth to generate a facial measurement, and compares the generated measurement to those already in the database to search for a potential match.

Facial recognition tools improve by training the AI through a process called machine learning. Facial recognition developers create a program that recognizes landmarks within a face, such as the tip of a nose or the center of an eye, and then calculates the distances between those landmarks. The program saves these calculations in a template, which is represented as a sequence of characters and numbers. Each template is unique to the program that created it and cannot be reverse engineered to re-create the submitted image. During the training process, the facial recognition program will compare each template to a set of training images annotated by the AI's developers. The program makes a hypothesis about the similarities between the two images, and the developers then confirm whether the hypothesis was correct. Through this process, the AI gradually learns what makes two images similar or different from each other. As noted in the

Accuracy Rates section below, there are widely accepted scientific processes to confirm that a facial recognition program is functioning reliably and accurately.[1]

When developers have determined an AI has consistently and successfully matched images, it can then be used to compare a submitted image to images on file. The facial recognition technology can be used to verify that an individual in a submitted image is the same individual depicted in a facial verification (a 1:1 match), image comparison (2-photo submission) or to identify an unknown individual by querying an entire gallery of images in a database to find an image similar to a submitted image (1:many match or identify candidates). Facial recognition algorithms are developed for particular uses by their developers and an algorithm's accuracy, functionality, or use cases will be highly contextual. For example, some facial recognition technologies are used in mobile phones and cameras to detect faces in a photograph but are not accurate enough to identify an individual. Similarly, a facial recognition technology employed by a phone manufacturer may be accurate enough to provide access to that phone but would not be reliably accurate to use in a law enforcement context.

As with any AI application, the accuracy of a facial recognition algorithm directly correlates with the breadth and quality of the data on which it is trained. Contextual factors may include the demographic of the population, camera quality, the rate of throughput, lighting, distance, and size of the database, as well as other factors.

Facial recognition algorithms must be trained with a diverse population of images to minimize misidentifications across all demographics of the population (e.g., age, gender, race). If developers have a large and diverse pool of training data, these programs are then more likely to create accurate hypotheses across races, ethnicities, and ages.[2]

Additionally, as a comparison tool, facial recognition operates with greater accuracy when there are fewer variables between pictures. This often requires ensuring that lighting conditions in the submitted image are similar to those in which the compared images were taken. Additionally, angles or distances between a subject and a camera should be similar. "Constraining" an image reduces variables by requiring that similar poses, expressions, lighting, and distances be adopted across images. Common examples of constrained images are mugshots and visa photographs. Photographs that are unconstrained, or taken "in the wild," such as images derived from surveillance activities or pulled from social media, are at a greater risk for inaccurate matches.[3]

Moreover, facial expressions, aging, and the obscuration of an individual's face by glasses, hats, and facial hair can further reduce the effectiveness of facial recognition. For this reason, the

[1] For more information *see* https://fiswg.org/index.htm.
[2] For more information *see* NIST, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects" (Dec. 2019) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.
[3] For more information *see* NIST, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" pg. 5. (Nov 2018) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

effectiveness of using facial recognition on an unconstrained image may vary based on seasonality (e.g., lower light levels and more individuals wearing hats or scarves in winter) or regional and cultural norms. Recognizing this factor, some FRSs have worked to create specialized algorithms that perform better on unconstrained facial images. While tending to be significantly slower and requiring computational resources than algorithmic models focused on constrained facial images, these FRSs provide greater accuracy when comparing unconstrained images.

Accuracy Rates

Accuracy rates are measures of the algorithms' efficacy by either the AI developers or an outside validator, such as the National Institute for Science and Technology (NIST). Accuracy rates are measured by how often the AI made the wrong hypothesis. An algorithm can be wrong in one of two ways: either guessing that images of two different individuals are the same person (false positive or false match) or guessing that two images of the same individual were not the same person (false negative or false non-match). While false non-match rates lower the efficacy of a facial recognition technology for HSI investigations, an algorithm's false-match rate has the greatest impact on individual privacy. ICE is working with the DHS Directorate of Science and Technology (S&T) on establishing an image quality capture standard to ensure consistency in data definition and accuracy for its use of facial recognition services.

Similarity Scores/Confidence Levels

A similarity score, sometimes known as confidence level, is a measure by the algorithm for how alike two compared images may be. A similarity score is different than an accuracy rate. Similarity scores are the statistical probability determined by the algorithm that an individual in a returned image is the same individual as the one in a submitted photo.[4] Similarity scores can be used as a threshold and are adjustable by a user. Setting a low similarity score threshold allows the algorithm to return larger sets of images from its gallery but increases the number of individuals who are likely not matches to the submitted image. For example, a similarity score set at a threshold of 85 will return all images that have an 85% or greater likelihood to be the same individual as one whose image has been submitted for identification. The algorithm generates a list of potential candidates, one of whom may match the submitted image. The user reviews the candidate list to determine if there is a successful match. In instances where a technology returns a list of candidates instead of an individual the facial recognition technology will always have a 100% error rate (deemed a false match rate), in that it will always return individuals who are not the individual depicted in the submitted image. The larger candidate lists, however, reduce disparate impacts of inaccuracy in the technology since it becomes more likely the correct

[4] McLaughlin, Michael & Castro, Daniel, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist" (Jan 2020) *available at* https://itif.org/sites/default/files/2020-best-facial-recognition.pdf.

individual is in a return and reduces the persuasiveness of an algorithmic return by showing multiple individuals that may share different biometric traits.[5] For example, an individual may share the same eye features with one individual, but the same nose landmarks as a different individual. As candidate list sizes grow, so does the amount of shared biometric traits across the return. The candidate list then becomes less certain. Candidate lists of any size require the user to complete additional steps (manual examination of the images or further investigation) to verify a match.

Candidate returns can also be set by a pre-determined list size. In these instances, the facial recognition service could return the number of most likely matches in the gallery, regardless of the statistical likelihood any will match. There is also the possibility that a service allows a user to set both a confidence threshold and list size. For example, a user may request a candidate list of 20 individuals with highest similarity scores unless a candidate's score is below 50%. This allows for the service to return large candidate lists, but reduces the likelihood of returning irrelevant candidates to a user. HSI will opt for a candidate list when using an FRS, and if possible, choose a candidate list length that is considered as best practices by law enforcement at the time of the query (e.g., 20 candidates) unless mission needs require a different number.

Facial Recognition Services

This PIA will focus on HSI's use of facial recognition services (FRS).[6] An FRS is a government agency or commercial vendor managing its own image databases and choosing its own facial recognition technology. Those agencies and vendors accept facial images from third parties, including HSI, to run comparative queries of its own image galleries using its own facial recognition algorithm. Examples of the types of FRS's that HSI uses are listed below.[7]

HSI uses an FRS's 1:many query functionalities to generate candidate lists to identify an unknown person or to locate a known person who may be using an alias or assumed identity. These requests are made in furtherance of ongoing investigations on a case-by-case basis.[8] ICE HSI

[5] For more information *see* NIST, "Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification" (Nov 2018) *available at* https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf.

[6] This PIA does not contemplate HSI owning or operating an algorithmic matching technology to run image searches against its own database. Within the Victim Identification (VID) Program algorithmic image matching is used to manage the National Child Victim Identification System 2 (NCVIS2), which is HSI's repository for all images and videos related to child exploitation material. No other PII is associated with images in NCVIS2 and the process is used to link cases. For more information *see* DHS/ICE/PIA-010 NCVIS *available at* www.dhs.gov/privacy. Any future acquisition or development of a facial recognition program by ICE will be covered in a separate PIA.

[7] *See* "Types of Facial Recognition Services used by HSI" section.

[8] This pertains to HSI making requests to FRSs, and not automated multi-modal biometric queries that may occur upon the enrollment of an individual in a biometric database. Further, this does not pertain to partner agencies running facial recognition queries as part of their own processes in a joint investigation in which HSI may be a partner.

primarily uses this law enforcement tool to identify victims of child exploitation and human trafficking, subjects engaged in the online and sexual exploitation of children, subjects engaged in financial fraud schemes, identity and benefit fraud, and those identified as members of transnational criminal organizations. HSI minimizes the privacy impacts of using an FRS through safeguards it has instituted at each step of the identification process. This process includes the initial collection of probe photos,[9] the submission of probe photos to the FRS, and the receipt and use of candidate lists from an FRS. Further, HSI does not take enforcement action against any individual solely based on candidate images. Rather, HSI uses these candidate images as leads, which always requires further corroboration and investigation.

Collection of Probe Photos

ICE uses an FRS by submitting facial images called probe photos. Probe photos must be directly relevant to an investigation and are only submitted to an FRS to further an active investigation. HSI collects a range of photographs during routine investigative activity including mugshots, surveillance photos, social media posts, and images confiscated from phones or other data devices. HSI may also isolate still frames from videos or streaming media to create a probe photo. Any of these sources can be used to isolate a facial image and create a probe photo.

HSI may collect constrained images and use an FRS to verify the asserted identity of an individual in limited circumstances, such as in suspected identity fraud cases. For example, HSI may submit a passport photo to an FRS to determine if that individual is linked to other names/identities held by that FRS.

The majority of images collected by HSI will be "unconstrained." Unconstrained images, often derived from surveillance activities or pulled from social media, inherently do not have the same controls on variation as constrained images. Some variations, however, can be reduced when the HSI agent collects/chooses the photo and isolates the facial image from the photo. The HSI agent will select isolated images that are best suited to be probe photos for the facial recognition processes. The HSI agent will ensure he or she isolates the facial image with the highest image quality possible, containing the fewest obstructions to the subject's face, and is most similar to a constrained image with regard to variables such as angle, lighting, distance, and subject expression. HSI endeavors to isolate images as similar as possible to those maintained in the galleries of an FRS (such as mugshots or passport photographs) to increase the likelihood of accuracy.

HSI safeguards prior to using Facial Recognition Services

Prior to submitting an image to an FRS, the HSI agent assigned to the case must first make reasonable efforts to identify the individual through existing means and methods. The agent must use reasonable efforts to identify the individual through government database queries, open source

[9] Probe photos are facial images that are lawfully obtained pursuant to an authorized criminal investigation and submitted for facial recognition matching.

research, and other conventional investigative techniques based on biographical and other non-biometric information prior to submitting a probe photo to an FRS. The agent's use of existing processes must be noted in the ICE Investigative Case Management System (ICM)[10] as a Report of Investigation (ROI). This documentation may occur after a query is conducted but must be completed prior to generating any lead for further investigation (see below).

HSI agents may only use an approved FRS for facial recognition identification. The approval process for an FRS can either be accomplished on a case-by-case basis at the HSI supervisor level or an FRS can be approved for HSI-wide use by the HSI Operational Systems Development and Management unit (OSDM). The mission of the OSDM is to coordinate development of new information technology (IT) systems, maintain existing IT systems, and identify new technologies for HSI. An HSI agent may submit an FRS to OSDM for inclusion onto a list of approved FRSs. OSDM will then evaluate the FRS to ensure that methods of transmission of the probe photo are properly encrypted, the FRS has the appropriate safeguards for housing sensitive PII, and the FRS does not retain or re-disseminate HSI probe photos. OSDM will consult with ICE Privacy, ICE attorneys, and other stakeholders throughout the evaluation process. OSDM will leverage resources such as NIST's Face Recognition Vendor Test (FRVT)[11] to evaluate the accuracy and bias of an FRS. Additionally, OSDM will conduct non-scientific tests of the FRS to gain insight into the veracity of the service. These evaluations will be necessary for approval by OSDM, but will not add weight to an FRS's returns. All returns will only be treated as investigative leads by HSI.

If an FRS is not pre-approved by OSDM and exigent circumstances dictate that the FRS must be used prior to OSDM review, the HSI agent must seek HSI supervisor approval prior to sending a probe photo. The HSI supervisor will confirm the exigent circumstance and ensure that the FRS is relevant and necessary for the investigation. The HSI supervisor will then submit the FRS to OSDM for review. The HSI supervisor will not evaluate an FRS's algorithm for accuracy or bias, as he or she does not have the technical capacity to comprehensively assess facial recognition technologies. OSDM will conduct a review of the FRS that was used and will ensure that the probe photo was not retained or reused by the FRS outside of the HSI-requested query.

When the HSI agent submits the probe photo, the agent notes the agency or vendor providing the FRS as part of the ROI in ICM. HSI supervisors are required to perform a review of agent submissions to FRS's on a periodic basis. HSI supervisors review ICM and the relevant case file to ensure agents use FRS's by the terms outlined in this PIA.

[10] *See* DHS/ICE/PIA-045 Investigative Case Management System (ICM) *available at* www.dhs.gov/privacy.
[11] For more information *see* https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt.

Submission Process to a Facial Recognition Service

HSI uses FRS databases that are open to federal law enforcement. Each FRS is entirely overseen and operated by the agencies and vendors that possesses the image galleries. HSI agents will either submit the probe photo manually to the FRS (e.g., via encrypted email) and a representative of the FRS will then input the image into their database to use the facial recognition technology, or will upload the photo directly to the FRS via a web interface.

HSI, through the Repository for Analytics in a Virtualized Environment (RAVEn) system,[12] will also develop a connection with OSDM-approved FRSs for HSI agents to submit probe photos. This will allow HSI to format probe photo submissions to the American National Standards Institute (ANSI)/NIST Type 10 record format for data exchange,[13] as well as to log and track all submissions by HSI and all returns by FRSs to ensure adequate security of the data and oversight of the use of FRSs. When this capability is developed, ICE Privacy will note the functionality in an update to the RAVEn PIA appendices.

HSI will only supply the minimum information required by the FRS to run the query. Usually this will only be the case agent's information and the probe photo itself. Some government FRSs may require the statutory authority or suspected crime to be submitted as well. For purposes of individual privacy and investigative case integrity, HSI will refrain from submitting more data than needed to the FRS.

In instances in which HSI may need a facial recognition service to verify the claimed identity of an individual during an investigation, HSI will request a 1:many query, as opposed to 1:1 verification. As discussed below, the impact of inaccuracies or biases in an FRS algorithm is reduced by returning a candidate list instead of a positive identification.

For instances like identity fraud, in which HSI requires facial recognition processes to assist with facial image comparison (2-image submission), HSI will only submit probe photos to an OSDM-approved FRS.[14] The submission and receipt process will be similar to a 1:many query request, but HSI will instead receive only a similarity score of the two photos from the FRS. For example, HSI may ask an FRS to determine the likelihood that an image in a passport photo matches the image in a photograph taken during the course of a law enforcement investigation. No PII will be returned as an output of an image comparison. The HSI agent may, if needed, submit a request to a relevant and necessary FRS for leads to the actual identity of an individual.

---

[12] *See* DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment (RAVEn) *available at* www.dhs.gov/privacy.
[13] ANSI/NIST ITL 1-2011, Update 2015, Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information, https://www.nist.gov/programs-projects/ansinist-itl-standard.
[14] *See* "Types of Facial Recognition Services" section below.

For a 1:many identity query HSI will only submit probe photos to an FRS whose query will not result in a single identity match, but rather in a candidate list of potential matches, which may be ranked by similarity scores.

This process generally works as follows:

- An HSI agent will come into possession of a facial image through existing investigative means and methods (e.g., via surveillance photographs, subpoenaed records, or identity documents); the image could be of individuals victimized by or suspected of committing a crime ICE has the legal authority to investigate.
- The HSI agent determines that use of the FRS is approved by HSI OSDM, is necessary, and is reasonably likely to result in a positive identification.
- If the FRS has not been previously approved, an HSI supervisor must approve the use of the FRS after ensuring that the circumstances require immediate submission to the FRS, and that the FRS will in turn be submitted to OSDM for further review as circumstances permit.
- If an FRS is approved, the HSI agent would submit the probe photo to the facial recognition service under the terms of service required by that agency or vendor and note the use of the FRS in ICM.
- The FRS will run a 1:many matching algorithm, by which it will compare the probe photo against its current galleries (e.g., mugshots and drivers' license records).
- The FRS will return a candidate list to the agent that may contain the similarity scores of each candidate. The candidate list may also contain any associated biographic information about a candidate currently contained within the FRS's database. The type of information will vary depending on the database (e.g., a law enforcement database may have derogatory information while a state Department of Motor Vehicles (DMV) database has driver records).

Some FRSs provide requestors the option of having their candidate lists reviewed by trained biometric face examiners. Face examination and reporting processes are based on best practices established by the Facial Identification Scientific Working Group (FISWG),[15] which operates under the NIST-run Organization of Scientific Area Committees (OSAC) for Forensic Science. The examiners will review algorithmic candidate returns using analysis of unique facial features called "morphological analysis."[16] In these instances the FRS technology will still provide a multiple candidate return, but the facial examiners provide an interim step of manual biometric

[15] For more information *see* https://fiswg.org/about_swgs.html.
[16] *See* FISWG Best Practices for Facial Image Comparison Feature List for Morphological Analysis, *available at* https://www.fiswg.org/FISWG_GuidelinesforFacialComparisonMethods_v1.0_2012_02_02.pdf.

analysis according to established industry standards and practices promulgated by the FISWG. If the FRS provides this option to HSI, then HSI may opt for the additional manual review. If HSI chooses to have returns analyzed, the examiner will provide HSI a narrowed candidate list, which may be as small as one individual. The examiner will also supply a confidence level score for each image returned, which is the examiner's explanation of the likelihood of a match between analyzed images. Manual facial examination by an FRS facial examiner is only a narrowing tool. It does not change the process by which HSI receives or uses returned images and does not provide add certainty that a match is contained in a candidate list that is returned.

Receipt and use of FRS Candidate lists for Lead Generation

Upon receipt of the candidate list, the HSI agent will compare the information returned by the FRS to other biographical and derogatory information in open source systems and governmental databases to determine if any matches are supported by corroborating evidence. This process is known as "vetting." HSI agents will not attempt to act as biometric face examiners and will instead compare candidate returns through non-biometric investigative processes. FRS similarity scores, if provided, will only be used as a triage tool for HSI vetting, not as an indicator of any criminal activity. To reduce any impacts caused by algorithmic inaccuracy or bias, HSI will not use an FRS return for 1:many queries that does not have a list of multiple candidates. If a multiple candidate return is narrowed to one individual by the FRS face examiner, HSI will still not consider the return a positive identification and will still vet the individual returned through open source systems and governmental databases. Similarly, HSI will only use an OSDM-approved FRS for 2-image photo comparison because the technology's accuracy and biases are continuously vetted by ICE subject matter experts.

An HSI agent will compare information received from an FRS to other information available to HSI from various sources to vet the potential match. Additional evidence leading to validation or elimination of a candidate as a possible match could include: biographic information, current and previous addresses, telephone numbers, vehicles, criminal history, immigration history, and information derived from publicly available social media. Candidate lists will be maintained in an external investigative case file as required under the Federal Rules of Evidence, or any other applicable statute, regulation or policy,[17] but non-vetted candidate information will not be used for leads or entered in an ROI in ICE systems and cannot be queried by ICM or other ICE systems.

If a candidate returned from the FRS is successfully vetted, the HSI agent will work up a lead for further investigation. Any lead related to a case is entered into ICM as a Report of Investigation (ROI). The fact that a lead was derived from an FRS generated candidate list will also be noted in the ROI, including the name of the FRS (e.g., name of the state DMV, name of

[17] *See* https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.

the commercial vendor source). HSI submits probe photos to FRSs for the purposes of establishing investigative leads. Leads are information with varying levels of credibility and will never be the sole basis used to establish probable cause, determine wrongdoing, or deny a benefit. FRS returns are generally accompanied by a disclaimer reminding the recipient that FRS processes are for lead generation purposes only and do not produce a product of sufficient weight to be used solely for a law enforcement action. For example, DHS's Office of Biometric Identity Management (OBIM) FRS returns the following disclaimer:

"OBIM Disclaimer: The images and information contained in this candidate list are for investigative lead purposes only, are not to be considered as positive identification, and are not to be used as the sole basis for any law enforcement action. Other information must be examined and considered prior to making a determination regarding the true identity of the individual in the submitted probe photo."

These disclaimers are produced by all federal FRSs used by HSI and ICE Privacy is required to screen new procurements before ICE purchases a commercial vendor FRS license. HSI will endeavor to ensure an FRS includes a disclaimer with a return prior to use, but if a candidate return is not accompanied by the disclaimer, HSI policy is to still treat all FRS returns as leads only.

Leads are only a first step in an investigative process of identification. Leads can come from any source and have varying levels of credibility. HSI agents routinely deal with leads during their day-to-day operations and are trained to validate or disprove leads through existing investigative methods. As an example, HSI operates a tip line to generate leads that averages 15,000 calls a month.[18] Similar to receiving a tip line lead, HSI agents are instructed that any vetted FRS candidate match must be further investigated by the HSI agent receiving the lead prior to ICE taking any enforcement action against an individual.

HSI agents who use an FRS must be able to testify to the use of facial recognition capabilities as other agents routinely testify regarding other biometric collection methods. HSI is developing, in consultation with ICE Privacy and S&T, a training on the processes and efficacy of facial recognition. If a lead is created from a vetted match and is then combined with other evidence to create probable cause, an agent may be required to testify to his/her use of an FRS in a judicial or administrative court. The HSI agent will also use such information in affidavits for warrants to explain how an agent initially identified a subject. A judicial court would then review the affidavit to ensure the veracity of the information prior to issuing the warrant. If a case is brought to trial,

[18] The HSI Tip line Unit is a 24-hour, seven days a week operations center. The Unit supports ICE's intake of and response to reports of suspicious activity or suspected illegal activity made by members of the public and other law enforcement agencies. For more information *see* DHS/ICE/PIA-033 FALCON Tipline *available at* www.dhs.gov/privacy.

information related to HSI's use of the FRS would be discoverable pursuant to normal judicial procedures.

Types of Facial Recognition Services used by HSI

FRSs are generally capabilities that were added to pre-existing biometric databases or criminal justice systems. The relevance of any particular FRS to an HSI investigation could be dependent upon the geographic location of the investigation, the type of investigation being conducted by HSI, and the type of image gallery the FRS contains. For example, an HSI agent would not submit a probe photo to an FRS run by a local police department in Florida if the crime being investigated took place in the state of New York, unless evidence or mission need dictated otherwise. Similarly, an HSI agent would be directed to first submit probe photos to the Department of State (DoS) Consular Consolidated Database (CCD) to determine if a passport or visa was fraudulent. Below are examples of the types of FRSs used by HSI. The list of FRSs is not exhaustive but will be updated in a PIA update if HSI uses an FRS of a significantly different type.

State and Local Facial Recognition Services

Many state and local law enforcement agencies (LEAs) throughout the United States have large databases of images collected during law enforcement actions (i.e., mugshots). Some of these agencies also connect directly to their associated DMV databases to allow for biometric querying of DMV information. It is common practice within the law enforcement community for LEAs to share information or allow other LEAs to submit biographic, descriptive, or other information in order to query their system. Many LEAs have now developed a service allowing external LEAs to submit probe photos to generate candidate lists from their databases for identification.

These state and local LEAs are geographically based and contain information collected within a particular locality. HSI would only submit probe photos to a state or local LEA if the agent had reason to believe the subject of the photo lived, visited, or had some other connection to that geographic location. The submission process for probe photos will vary by each LEA but generally follows the same process by which an HSI agent may request a biographic check for the subject of an investigation. Some states have granted HSI offices within their regions access to submit probe photos directly to the FRS. OSDM will review the terms and conditions of a new state or local FRS to ensure proper handling and safeguarding of HSI images. This will occur prior to submission of probe photos, except if an exigent circumstance requires immediate submission, then OSDM will review the terms and conditions as soon as possible thereafter. Regardless of the circumstances, any HSI user who wishes to access a state or local FRS must sign the FRS terms and conditions of service prior to accessing the service.

The number of candidates returned from a LEA FRS will vary as well as the type of biographic information returned with the list. If a LEA only queries a criminal database, then biographic and derogatory information would be returned to HSI. If the LEA connects to a state

DMV database, then a candidate's associated driver's license information could be included and driving records could also be accessed by HSI upon request.

Regional and subject matter-specific intelligence fusion centers

Transnational crime and criminal organizations expand beyond local or state jurisdictions. As such, many law enforcement agencies have partnered to create intelligence sharing centers (also called fusion centers) to collaborate and deconflict law enforcement activities regarding specific crimes (e.g., drug trafficking, human trafficking).[19] Fusion centers act as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal, territorial, federal, and private sector partners. HSI is a partner in many fusion centers whose mission aligns with HSI's statutory authorities so that HSI can track criminal activities, including those involving gangs, reported within a region.

Certain fusion centers have data analytic capabilities that aid investigators in processing and visualizing evidence. One capability that certain fusion centers are developing is an FRS to query their subject-specific galleries. Fusion center users can submit a range of photographs collected during law enforcement activities. This results in a repository of individuals identified as suspected of participating in a criminal organization for later use by the fusion center. The galleries are narrowly focused and directly relevant to HSI's queries.

If ICE is a partner in the fusion center, then HSI agents can submit probe photos of suspects. The center's FRS will run a matching algorithm that will compare the probe photo to its current gallery of known or suspected criminals. The FRS will return a candidate list from the gallery to the agent with a similarity score indicating the likelihood of identification to the probe photo.

The candidate lists will contain any information about a candidate that is currently contained within the fusion center. This could include biographic information, derogatory information, criminal intelligence, and known associates. Any information or connections made between submitted photos and entities within the fusion center must be manually entered by a fusion center user.

Federal Agency Facial Recognition Services

DHS Office of Biometric Identity Management (OBIM) Facial Recognition Services

OBIM's authoritative biometric database, the Automated Biometric Identification System (IDENT), is the central DHS-wide system for the storage and processing of biometric data.[20] This will change as OBIM completes its modernization by deploying the Homeland Advanced

[19] https://www.dhs.gov/fusion-centers.
[20] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT) (December 7, 2012), *available at* https://www.dhs.gov/privacy.

Recognition Technology (HART) system.[21] IDENT/HART stores and processes biometric data—digital fingerprints, facial images (photographs), and iris scans—and links biometrics with biographic information to establish and verify identities. OBIM serves as a biographic and biometric repository for all of DHS.[22] OBIM is in the process of connecting to FBI's Next Generation Identification (NGI) System, the Department of Defense's Automated Biometric Identification System (ABIS), and the Department of State's Consolidated Consular Database to enable requests for facial recognition queries through IDENT/HART.[23] OBIM identifies each collection by data provider and its authority to use, retain, and share data. IDENT can restrict queries of its database on request of the data provider and only enables sharing with authorized users after the data provider has approved the sharing. HSI agents may submit probe photos to IDENT/HART manually through OBIM's Biometric Support Center (BSC) or through a submission portal that is being developed on HSI's RAVEn platform. HSI will ensure that the BSC will delete probe photos after a query has been processed.

The output of an OBIM 1:many face query is a candidate list (a rank ordered list of the highest scoring comparisons above a preset threshold) of those images that data owners have permitted to be shared for this purpose. The length of the candidate list is selected by HSI. HSI will choose a list length that is considered best practice by law enforcement. HSI agents can access from an OBIM FRS query: biometric data; personal information (names, dates of birth, gender, etc.); personal identifiers (e.g., Alien number, Social Security number); biometric administrative identifiers (Federal Bureau of Investigation (FBI) Fingerprint Number -Universal Control Number (UCN), IDENT Fingerprint Identification Number (FIN), Department of Defense (DoD) Biometric Identity Number (BID)); personal physical details (e.g., height, weight, eye color, and hair color); identifiers for citizenship and nationality; derogatory information, if applicable; contact information; and encounter data.

Prior to HSI receiving the candidate list, the HSI agent can request the OBIM BSC provide examination. Trained BSC face examiners closely compare the probe photo against each of the candidate face images to determine if any of them are the same individual. Once results are verified, the BSC returns either a no-match or only those candidate(s) assessed to be likely matches. The return of a likely match will not be noted in IDENT/HART. If HSI validates a

[21] The migration from IDENT to HART operations occurs in phases to minimize impact to OBIM's mission partners. The migration will occur without unscheduled interruption of service delivery to OBIM's mission partners, with minimal scheduled service outages, and without degradation in service levels (response time) to those partners.
[22] *See* DHS/OBIM/PIA-004 Homeland Advanced Recognition Technology System (HART) Increment 1 PIA, *available at* www.dhs.gov/privacy.
[23] NGI, ABIS, and CCD databases, and cites to appropriate privacy documentation, are discussed in this section below.

candidate as a match it is the responsibility of the HSI agent to update any information in IDENT/HART through existing methods after a candidate has been vetted and a lead validated.

Department of State (DoS) Consular Consolidated Database (CCD)

CCD is the DoS repository for all visa and passport records.[24] It is used not only by the DoS as part of the visa adjudication process for biographic and biometric checks but also by DHS, the Department of Defense, and the Federal Bureau of Investigation (FBI). The CCD stores information about U.S. citizens and Lawful Permanent Residents (LPRs) who have filed for passports. It also contains information on foreign nationals who have filed immigrant and non-immigrant visa applications. CCD may also contain additional information stored submitted by federal agencies as a result of background checks on the individual. The CCD provides an FRS comparison against their database of visa records. An HSI agent may submit a probe photo to a CCD user to determine if an individual is in the database. CCD does not retain probe photos.

The candidate list will return all information associated with the individual contained within CCD. PII in a candidate return will only include matched images from visa and passport photos contained in CCD. HSI must then make a secondary request through the DoS Bureau of Diplomatic Security for additional information on an individual. This information could include biographic information, immigration information, contact information, financial information, medical information, legal information, educational information, biographic information on family and associates, derogatory information, and social media information (e.g., usernames listed on a visa application).

FBI Next Generation Identification System (NGI) Interstate Photo System

NGI is the FBI's primary identity management system. It contains biometric and criminal history records submitted to the FBI for criminal justice, national security, and civil purposes. The system has over 38 million criminal photos that are associated with a 10-print fingerprint scan.[25] NGI provides a facial recognition query capability to domestic law enforcement agencies to compare probe photos to its criminal photo gallery. Currently, before ICE can query NGI galleries via facial recognition, an HSI agent must open a cooperative case with the FBI, meaning that ICE and the FBI collaborate regarding an investigation that may implicate both agencies' statutory authorities. ICE would share the images with the FBI field office assisting with the case, and an agent from the FBI would submit the request for a query of NGI. All photos stored in the FBI NGI databases must be associated with a ten-print fingerprint. FBI will not maintain probe photos within NGI because probe photos are not associated with fingerprints. Probe photos may be

[24] *See* https://2009-2017.state.gov/documents/organization/242316.pdf.*See also* https://2001-2009.state.gov/documents/organization/109132.pdf.
[25] *See* https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

retained, however, in the FBI field office case file for investigative purposes.[26] NGI will always return multiple candidates from a query; anywhere from two to 50 photos may be returned. The ICE user submitting the probe photo can designate the number of candidates to be returned. The number of candidates may differ based on mission need, but HSI agents will be instructed to select a number that is considered best practices by law enforcement (e.g., 20 candidates) by default.

HSI also has the ability to request that the FBI field office use the FBI's Face Analysis, Comparison, and Evaluation (FACE) services unit.[27] This unit has trained facial examiners similar to those at OBIM who will manually review candidate lists generated by the algorithm to identify the most likely matches and ensure the quality of the candidate list.

Department of Defense (DoD) Automated Biometric Identity System (ABIS)[28]

ABIS is DoD's authoritative biometric system for matching, storing, and sharing biometrics in support of military operations. ABIS contains information on known or suspected terrorists, individuals deemed national security threats, DoD detainees, and individuals of interest to DoD. ABIS shares information with other federal agencies and DoD's foreign partners. ABIS has the functionality to conduct facial recognition queries. In the future, HSI may submit probe photos through IDENT/HART's connection with ABIS.

ABIS encounter information could contain data elements such as: ABIS encounter specific identifier, reason fingerprinted, date fingerprinted, associated derogatory information, the fingerprinting agency, associated biometrics (e.g., fingerprints), name, aliases, date of birth, place of birth, country of citizenship, and gender.

Commercial Vendors

Some commercial vendors maintain their own repository of images collected from either their own processes or searches of open source systems, obtained by "scraping" internet websites.[29] The images are unconstrained and may include multiple individuals. All collected images are available to the public. Vendors collect all images via simple searches. While HSI cannot directly control the means or methods of a vendor's data collection efforts, if HSI discovers that an FRS

[26] For more information on FBI case file retention and management *see* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/sentinel.
[27] *See* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit.
[28] For more information *see* Defense Biometric Services, 74 FR 48237 (Sep. 22, 2009), available at http://dpclo.defense.gov/privacy/SORNS/dod/A0025-2_SAIS_DoD.html, and Department of Defense Detainee Biometric Information System, 72 FR 14534 (Mar. 28, 2007), available at http://dpclo.defense.gov/privacy/SORNs/dod/A0025-2c_SAIS_DoD.html. DFBA policy on biometrics are *available at* https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/852101E.pdf.
[29] Scraping is an automated process that retrieves websites, searches for and copies data that has been pre-designated by a user, then loads the copied data into a database for later use.

violates the privacy settings of an open source system, HSI will discontinue using that vendor's FRS.

Commercial vendors have also created facial recognition algorithms to query their proprietary databases. HSI has purchased licenses and/or paid for access to the FRSs of these vendors. HSI may upload an image to the vendor and require the vendor to delete the image immediately upon creation of a face template. A vendor may also provide a facial recognition query to compare one image in the vendor's database to other images in its database. In those instances, HSI will not upload any probe photos, but will select an image that was returned by conventional query method of the vendor's holdings (e.g., name search) and the vendor will use facial recognition technology to search for similar images.

The vendor's facial recognition technology will use available data to find images in its compiled dataset that match or are similar to the probe photo HSI uploaded or selected from the vendor's gallery. The vendor's technology will search all images in its gallery and all individuals that may be contained within an image in its gallery. If a vendor matches a candidate within an image containing multiple individuals, the vendor will isolate the facial image of the matched candidate within the candidate list. Therefore, HSI will only receive responses containing matched individuals. The returns are rank ordered so that images with the highest confidence scores are returned first. If an HSI agent is given the option by the vendor, he or she will opt for a limited number of returns (e.g., 20 candidates) rather than setting a confidence threshold.

The vendor will display any information it may have in its database associated with the image. Typically, this will include a link to the URL where the image was found so the investigator can go directly to the open source site. HSI would then capture and store relevant information obtained through the source URL. HSI agents will thoroughly check information derived from the open source site against government and public databases to either confirm or eliminate candidates prior to generating leads to send to the field for additional investigation.

Vendor facial recognition queries are treated as equivalent to open web searches via a search engine. HSI will not save the entirety of returned query results in ICE systems. Rather, HSI will only collect and document salient results as they pertain to the investigation.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[30] 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 personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure

[30] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[31]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[32] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208[33] and the Homeland Security Act of 2002 Section 222.[34] Given that HSI's use of facial recognition services spans multiple programs and activities, rather than comprises a singular information technology system, this PIA is conducted as it relates to the DHS construct of the Fair Information Principles. This PIA examines the privacy impact of Facial Recognition Services operations as it relates to the Fair Information Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

Notice of the existence, contents, and uses of FRSs by HSI is provided by the publication of this PIA and by the DHS/ICE-009 External Investigations System of Records Notice (SORN).[35] Since an FRS is a law enforcement tool that HSI uses to process sensitive information related to criminal investigations, it may not be feasible or advisable to provide notice to individuals at the time their image is collected or submitted as a probe photo. Some probe photos may be collected through other lawful means, such as by subpoenas and search warrants, and the record holder of those images are notified of the collection. If images are obtained from individuals through Federal Government-approved forms or other means, such as information collected pursuant to seizures of property, notices on the relevant forms generally state that the information may be shared with law enforcement agencies.

---

[31] 6 U.S.C. § 142(a)(2).
[32] *See* Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* www.dhs.gov/privacy.
[33] 44 U.S.C. § 3501 note.
[34] 6 U.S.C. § 142.
[35] DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010). This SORN is currently in the process of being updated.

Privacy Risk: There is a risk that an FRS will not provide adequate notice that its biometric collections may be used for facial recognition matching.

Mitigation: The risk is not mitigated. It is incumbent on the FRS to provide notice that images collected from individuals will be subject to facial recognition matching. Many FRSs use photographs collected for law enforcement purposes and background checks, such as mugshots and visa photos. These photos are collected directly from an individual and they are notified that the information can be used for law enforcement purposes. Some FRS galleries, such as DMV photographic galleries, collect photographs for purposes unrelated to law enforcement, but notify individuals generally that information collected could be used by law enforcement. However, HSI does not control the notice an FRS provides to individuals at the time of collection and cannot notify an individual when its agents use an FRS without informing a criminal suspect of an active investigation.

Privacy Risk: There is a risk that ICE uses unconstrained images and individuals will not have notice their image was used as a probe photo or that their information was obtained by HSI through an FRS.

Mitigation: This risk is being mitigated. Suspects in probe photos or identified via FRS data may not be advised they are being investigated. Notice to these individuals could inform them that they are the target of an actual or potential criminal investigation or reveal investigative interest on the part of DHS or another agency. Access to the records might also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, harm victims, or to avoid detection or apprehension.

All individuals present in the United States, however, have constitutional protections in criminal proceedings entitling them to discovery production.[36] The discovery obligations of federal criminal prosecutors are generally established by the Federal Rules of Criminal Procedure 16 and 26.2, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*,[37] and *Giglio v. United States*.[38] In immigration proceedings each party is responsible for producing evidence upon which it seeks to rely in the litigation. Therefore, if ICE seeks to use information derived from an FRS to sustain any charge or otherwise as evidence, it would produce that information.

[36] Discovery is the general process of a defendant obtaining information possessed by a prosecutor regarding the defendant's case.
[37] 373 U.S. 83 (1963).
[38] 405 U.S. 150 (1972).

2. Principle of Individual Participation

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

HSI will use an FRS when an individual cannot be identified or located via conventional investigative methods; therefore, the individual in question will generally not be able to individually participate in HSI's collection of probe photos or use of an FRS. In instances in which an individual participates in the collection of the photo (i.e., an individual suspected of identity fraud or whose phone contents are subpoenaed) there is no opportunity or right to decline to provide the images due to the law enforcement context in which probe photos are collected. These materials are potential evidence of criminal activity and are seized and used in accordance with criminal procedure.

FRSs that are maintained by federal, state, and local agencies generally collect images for their galleries directly from an individual. During the collection these agencies also collect biographic information from the individual that will be associated with the image. This includes consensual collections, such as images for state identification or visa applications, or non-consensual collections, such as mugshots. An individual does have the opportunity in most instances of consensual collections to opt out of having themselves photographed. However, they may then forfeit the ability to use the service (licensure) or benefit (visa) to which they applied.

Similar to notice, ICE does not control the access and correction procedures for FRSs. The ability for an individual to opt out of facial recognition queries or to access and amend information in a gallery is entirely dependent upon the FRS. All federal databases have access and amendment processes in place that are discussed in their relevant PIAs and SORNs.[39] State DMV databases similarly allow individuals to correct and update information online or in person at an office. An individual's ability to amend information in federal, state, or regional law enforcement information systems, however, is limited by law and policy due to the need to protect national security or law enforcement sensitive information.

For the same reasons, individual access to HSI holdings regarding probe photos, candidate returns, and/or vetting efforts are limited.[40] Individuals may submit requests for information and correction as permitted by the Privacy Act, and the requests will be reviewed and corrected on a case-by case basis. Individuals seeking to correct records, or seeking to contest their content, may submit a request in writing to the ICE Privacy and Records Office by mail:

---

[39] *See* footnotes 6-9.
[40] *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010), Final Rule for Privacy Act Exemptions, 74 FR 4508 (August 31, 2009).

U.S. Immigration and Customs Enforcement Privacy and Records Office
Attn: Privacy Branch 500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
(202) 732-3300
http://www.ice.gov/management-administration/privacy

Privacy Risk: There is a risk that individuals cannot access and amend inaccuracies in commercial vendor collections.

Mitigation: The risk is not mitigated. If a vendor FRS collects media from publicly available sources, any correction or update the individual makes to the information in the open source system might not be reflected in the vendor database. Moreover, vendors may not notify HSI when an update or correction occurs within its own proprietary database. HSI, however, will always research the source URL that originally contained information from a vendor FRS return to ensure that the information is as accurate, timely, and complete as possible prior to vetting a candidate and generating an investigative lead.

3. Principle of Purpose Specification

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

ICE is authorized to collect information under Section 701 of the USA PATRIOT Act; 6 U.S.C. § 112; 8 U.S.C. §§ 1105, 1103(a)(4), 1357(a) and (b); and Executive Order 13388. Pursuant to the Homeland Security Act of 2002 (HSA), as amended, Pub. L. 107-296, 116 Stat. 2135 §§ 102, 102, 403, 441 (Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include laws contained in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this enforcement authority to the Director of ICE in DHS Delegation Order No. 7030.2, Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (Nov. 13, 2004), and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003). This authority has been delegated to HSI through ICE Delegation Order 73005.1, Immigration Enforcement Authority of the Director of the Office of Investigations (Mar. 5, 2007). Through these statutes and orders, HSI has broad legal authority to enforce an array of federal statutes including responsibility for enforcing U.S. civil immigration authorities, customs authorities, and federal criminal authorities. HSI investigates all types of cross-border criminal activity, including financial crimes, money laundering, and bulk cash smuggling; commercial fraud and intellectual property theft; cybercrimes; human rights violations; human smuggling and trafficking; immigration, document, and benefit fraud; narcotics and weapons smuggling/trafficking; transnational gang activity; export enforcement; and international art and antiquity theft.

HSI will only submit probe photos to be used in furtherance of ongoing criminal investigations. Under this PIA, ICE's Enforcement and Removal Operations (ERO) will not use and HSI will not support ERO in using FRSs solely in furtherance of civil immigration enforcement. HSI will only submit probe photos that are linked to ongoing criminal investigations for crimes HSI has the statutory authority to enforce. ICE stores all probe photos and results of an FRS queries in an ICE system of records and maintains them in accordance with the Privacy Act of 1974.[41] HSI's collection, use, and maintenance of this information is covered under the DHS/ICE-009 External Investigations SORN.[42]

Privacy Risk: HSI may use an FRS for purposes beyond what is described in this PIA.

Mitigation: This risk is being mitigated through training and oversight. HSI, DHS S&T, and ICE Privacy will create a training and Rules of Behavior (ROBs) for HSI agents that details the restraints and safeguards outlined in this PIA. Federal and state FRSs also require that probe photo submissions be associated with an ongoing law enforcement activity by requiring the agent to state the violation he or she is investigating. Some commercial vendors also log FRS queries/returns and make those logs available upon request. ICE Privacy will only approve the use of a commercial vendor that provides auditing capabilities. HSI supervisors will regularly audit agent case files to ensure that the source of probe photos, the necessity and relevance of an FRS, the use of an FRS, and the name of the FRS are noted as an ROI in ICM. ROIs must be approved by a supervisor before they are considered final and available for viewing by other ICM users, ensuring that HSI supervisors will oversee agent use of FRSs. Candidate returns and leads generated will also be noted as ROIs within ICM. As such, accountability regarding the collection, sharing, and receiving of information in connection with an FRS will be similarly overseen and audited by HSI supervisors. Finally, ICM entries are routinely audited by the ICE Office of Professional Responsibility (OPR) to ensure proper use of the system and proper handling of evidence in investigations. Agents found to be mishandling evidence, including probe photos, face disciplinary action by ICE.

[41] 5 U.S.C. § 552a.
[42] *See* DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010). This SORN is currently in the process of being updated.

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).

HSI will extend its existing policies and oversight regarding evidence gathering and handling to its collection of probe photos to ensure only the minimum amount of data required for an investigation is collected. HSI agents only collect information in furtherance of their statutory law enforcement authorities for the purposes of furthering an ongoing investigation. Probe photos will always be obtained either via open source systems, government databases, or proper law enforcement requests and activities.

HSI will not collect probe photos from individuals actively exercising rights protected by the First Amendment to the United States Constitution (e.g., at religious services or political protests). During the FRS submission process, HSI will only create probe photos from individuals suspected of participating in or being victimized by a crime under its legal authority. HSI will only submit still images of a single face as a probe photo to an FRS. ICE Privacy, DHS S&T, and HSI are developing a training for HSI agents, in consultation with ICE attorneys and the DHS Office for Civil Rights and Civil Liberties, that will cover these restrictions on collections. HSI supervisors will also be trained to review FRS requests and ROIs by their agents to ensure adherence with these practices.

Probe photos and candidate returns will be maintained within the relevant case file. Case files are retained for 20 years after the case is closed in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B).[43] ROIs within ICM connected to the case will similarly be deleted 20 years after case closure. An ICE-wide updated schedule for investigative records is being developed and will be submitted to the National Archives and Records Administration (NARA) for approval.

Privacy Risk: An FRS may return excessive amounts of candidates, leading to an overcollection of individual information irrelevant to the ongoing criminal case.

Mitigation: The risk is being mitigated. Some FRS agencies and vendors allow a law enforcement agency the option of setting the maximum number of candidates to be returned from a query. If the FRS has the functionality, then the HSI agent will select as a default a number that is considered best practice by law enforcement (e.g., 20 candidates) returned per query. Returns should be large enough to reduce the impact of false positive matches from an FRS because it

[43] Records retention is made in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B), *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-the-treasury/rg-0036/n1-036-86-001_sf115.pdf.

increases the likelihood the correct individual is among the candidates. HSI vets multiple individuals to create a lead and HSI cannot rely on the match alone as verification that the candidate matches the probe photo.

If an FRS returns similarity scores with a candidate list HSI will use those scores to triage its vetting process. Candidates with low similarity scores may not be vetted if HSI can confirm an identity in a return. Only successfully vetted candidates will be entered into ICM as an ROI. Information regarding candidates returned by an FRS that were unsuccessfully vetted by HSI will only be maintained in the external case file at the local HSI office where the investigation is occurring per the Federal Rules of Evidence. That information cannot be searched by personal identifier and will not be used by HSI for any other purpose.

Privacy Risk: There is a privacy risk that information will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: The risk is mitigated. The 20-year retention period for ICM and other case file records is consistent with the retention schedules for other investigative records within DHS. By ensuring that information pertaining to individuals who are encountered repeatedly over a span of time can be linked, this retention period supports HSI's effective enforcement of U.S. civil immigration authorities, customs authorities, and federal criminal authorities. Closed cases can contain information that may be relevant to a new or existing case and need to be readily searchable and accessible for at least a period of time. The addition of probe photos and candidate returns to a case file will not affect the existing retention processes in ICE systems. Probe photos and candidate returns will be destroyed when the case file is destroyed.

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 use and sharing of probe photos by HSI will only be for purposes compatible with the original purpose for collection, which is to conduct criminal law enforcement investigations and other immigration enforcement activities, to uphold and enforce the law, and to ensure public safety. HSI limits the use of FRSs to ongoing investigations when conventional investigative means have been unsuccessful in identifying or locating a subject. HSI personnel will be trained so that they do not use an FRS to surveil the public. HSI agents do not have the capability and will not attempt to procure any device that allows an FRS to analyze live video, streaming media, or any other surveillance device in real-time.

All external sharing falls within the scope of applicable law, including the published routine uses in the DHS/ICE-009 External Investigations SORN, in particular routine use J, as any

FRS submission would be to third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation. HSI will ensure that probe photo use and disclosure is within the proper performance of the official duties of the agent making the disclosure.

Privacy Risk: HSI may submit images that are not directly relevant to an ongoing criminal case.

Mitigation: This risk is being mitigated. HSI personnel will receive training that details the appropriate uses of an FRS, including the requirement that all submitted images be relevant to an ongoing investigation. HSI agents will note the source of collection for probe photos in the investigative case file and as part of an ROI in ICM. HSI supervisors will review ROIs to ensure that probe photos were collected from an appropriate source for an appropriate purpose and the FRS used was necessary and relevant to further the investigation. ICM entries are routinely audited by the ICE Office of Professional Responsibility (OPR) to ensure proper use of the system and proper handling of evidence in investigations. Agents that are found to be mishandling evidence, including probe photos, face disciplinary action by ICE. Probe photos and resulting information that were inappropriately submitted or collected are deleted upon discovery of inappropriate conduct.

Privacy Risk: HSI may investigate candidates returned from an FRS who have not been properly vetted or are not linked to the probe photo.

Mitigation: This risk is being mitigated through auditing and oversight of HSI investigative activities. HSI supervisors routinely review their agents' case files and inspect generated leads as part of their review. Any lead received by an HSI program or office is routinely reviewed by an HSI Supervisor prior to assigning the lead to an agent to follow up. Ultimately, any investigative activity by an HSI agent must be entered into ICM as an ROI or a subject record. ROIs must be approved by a supervisor before they are considered final and available for viewing by other ICM users. In contrast, Subject Records created by ICM users are immediately viewable to other ICE users because of the need to deconflict them (and because of officer safety concerns), but they are flagged to indicate they are pending until a supervisor reviews and approves them. Copies of ICM records are not placed in the HSI Data Warehouse[44] until they are approved. HSI supervisors will ensure that HSI investigative activity is only conducted through appropriate means and will delete any records obtained improperly by an agent. Further, the agent may be disciplined for improper use of the FRS returns and referred to ICE OPR.

[44] The HSI Data Warehouse is a data storage environment that serves as a repository for ICM system data. It receives a direct feed once every 24 hours containing a refresh of ICM data, including new records and edits to previously existing records. For more information on HSI Data Warehouse *see* DHS/ICE/PIA-045 ICM.

Privacy Risk: An FRS may use images submitted by HSI for purposes other than its original collection.

Mitigation: The risk is being mitigated. HSI will review FRS terms of service and policies to ensure that all FRSs it uses, including commercial vendors, will not re-disseminate probe photos and will delete probe photos immediately after a face template is created. In cases of exigent circumstance where an FRS cannot be vetted prior to submission of a probe photo, HSI will engage with the FRS directly after the submission to ensure the submitted photo was deleted. The government agencies with which HSI engages for FRS have authorities and missions consistent and compatible with the authorities and mission of DHS, ICE, and HSI, thereby reducing the likelihood any agency uses a probe photo for purposes outside of law enforcement or public safety. Moreover, HSI will only send the probe photo of the subject without contextual information. The probe photo would be of limited value to the FRS without any associated information.

6. Principle of Data Quality and Integrity

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

Facial Recognition algorithms have become exponentially more accurate over the past decade. However, due to the novelty of the technology and potential for error, HSI only uses FRS returns as the first step in an investigative process. Results of FRS processes can vary on a case by case basis. This is because the accuracy of an algorithm used by FRSs varies among agencies and vendors and similarity thresholds are not standard across FRSs.

Moreover, the quality of submission by HSI agents can affect the accuracy and integrity of the FRS candidate returns. For example, the lighting, sharpness, and resolution of the image will all affect the accuracy of the FRS. Further, a subject's angle to the camera, expression, or occluding features (e.g., facial hair, sunglasses) will affect each FRS algorithm differently. DHS S&T will be working with HSI and ICE Privacy on proper collection and isolation techniques (e.g., zooming, cropping) to reduce variations between a probe photo and an FRS's image gallery.

As the variation in accuracy and biases in FRSs used by HSI cannot be controlled by ICE, HSI ensures that each candidate return from an FRS is given proper weight in the investigative process. HSI agents are continually trained to know that candidate returns are leads only, and not a positive identification. Candidate returns are not used as an indicator of unlawful activity or used to establish probable cause. HSI agents only use a vetted candidate match as the first step in the investigative process and are required to compile validating evidence of the match.

Privacy Risk: There is a risk HSI will submit low quality images or probe photos that would otherwise increase the likelihood of false matches from an FRS.

Mitigation: The risk is being mitigated. Most FRSs exercise quality control of images accepted into their systems. As the biometric service provider, the FRS can reject a probe photo that is of too low a quality to produce a candidate list to the designated confidence threshold. Some FRSs offer users specialized training that details proper collection techniques, selection criteria, and cropping techniques for probe photos for use of their gallery. As part of their terms of service, some of these FRSs require a requestor to certify that he or she has taken the training prior to submitting a probe photo or receiving access to upload probe photos. Additionally, ICE Privacy will be working with HSI and relevant stakeholders to develop a training HSI agents will take to maximize image quality prior to FRS submission.

Privacy Risk: There is a risk an FRS will misidentify individuals in the facial recognition process. This risk is increased because ICE may not have control over the accuracy standards or thresholds set by third party FRS technologies.

Mitigation: The risk is being mitigated. FRS technologies return lists of candidates and do not make positive identifications of any individual. Candidate lists reduce the impact of potential false positive matches by an FRS. This is because lists remove the certainty of positive identification on biometrics alone and requires HSI to vet multiple individuals to create a lead as different individuals may share different biometric traits. Therefore, HSI cannot rely on FRS results alone as verification that a candidate return matches the probe photo. In cases in which HSI requests review by a trained facial examiner, the algorithm will still return a list of multiple candidates, and a trained biometric examiner will act as a further check for accuracy against an FRS return. A return from a facial examiner will result in a smaller candidate list being returned from the FRS but will be accompanied by the same disclaimers stating that candidates must be vetted and that information should be used for lead purposes only. HSI will not use lists returned by an FRS for any lead or law enforcement action without additional research and analysis, even if a trained facial examiner from an FRS has narrowed the list to one candidate. HSI agents will cross check FRS returns against government databases and open source information, such as news articles or public records, to vet potential matches. Finally, possible matches are considered investigative leads until HSI agents gather additional evidence that validates the potential match.

Privacy Risk: There is a risk that HSI will use biographic or derogatory information received from an FRS that is inaccurate.

Mitigation: This risk is being mitigated. The original collection of the data by federal and state/local FRSs will be from the individual directly. Data returned by intelligence fusion centers are gathered for law enforcement and/or national security purposes. Law enforcement and national security personnel are trained to review all information they collect for accuracy, as errors may detrimentally affect prosecutions and investigations. This increases the likelihood that the information within a fusion center has been previously vetted for accuracy. Commercial vendor FRS returns link directly to the source material from which the data is collected, allowing HSI

agents to collect data directly from the source. Additionally, HSI will conduct its own research and investigation to determine if the information returned by an FRS is accurate before taking any enforcement action.

7. Principle of Security

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

The HSI office making an FRS request is responsible for the security of PII transmitted and received. HSI agents accessing an FRS follow ICE standard technical and organizational safeguards that protect against unauthorized disclosure, alteration, access, or use of PII and SPII. Each FRS will have its own procedures for submitting and receiving information. OSDM or an HSI supervisor must approve any FRS prior to HSI submitting probe photos. In that approval, OSDM must ensure that the FRS takes reasonable measures so only authorized individuals have access to the PII exchanged. OSDM will do this prior to a probe photo submission, or in the cases of exigent circumstances, as soon as possible thereafter. The agent and the supervisor will also ensure that transmission and receipt of information while using an FRS are appropriately encrypted in accordance with DHS standard operating procedures in the safeguarding of sensitive PII[45] and ICE standards on the handling of law enforcement sensitive information. OSDM will also check that the FRS's terms of service and data security polices state that it does not retain any probe photos sent by HSI or share probe photos with other parties.

Information retained by HSI, including probe photos and candidate returns, are secured through ICM. The ICM system actively prevents access to information for which a user lacks authorization, as defined by the users' need to know and job responsibilities. The user who created a case or record in ICM may limit the access by others to that information, except for the originator's supervisor. HSI agents are required to complete ICM-specific, role-based training before being granted an ICM account.

Privacy Risk: There is a risk that an FRS will mishandle HSI data, leading to a data breach or privacy incident.

Mitigation: This risk is being mitigated. HSI's submission to an FRS will only contain the minimum amount of information necessary for the FRS to run a biometric query. Usually this only involves the case agent name, the probe photo, and the statutory violation being investigated. If a breach occurs, the information lost by the FRS will be minimal and without context. OSDM will also ensure that the FRS's policies require it to delete the probe photo after its algorithm

[45] For more information *see* DHS Handbook for Safeguarding Sensitive PII *available at* www.dhs.gov/privacy.

creates a face template or finishes a search. All that would remain in an FRS database would be the case agent name and a log of the request itself.

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 should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

HSI's use of FRSs is an extension of its existing investigative processes. Therefore, the auditing and oversight of FRS use is in keeping with the handling of any sensitive evidence maintained in the HSI Investigatory Case Management system (ICM). The HSI supervisor will regularly audit investigative case files to ensure that the use of an FRS and the name of the FRS are documented as an ROI in ICM. Candidate returns and leads generated will also be recorded as ROIs within ICM. As such, accountability checks regarding the collection, sharing, and receiving of information in connection with an FRS is dependent on HSI agents following HSI standard procedures and requirements for logging information in the ICM case management system. Additional specifics regarding ICM's auditing and accountability procedures can be found in the ICM PIA.[46]

The access controls, auditing, and supervisory review of ICM case files ensure information is used in accordance with the stated practices in this PIA. The HSI case agent receives a query notification whenever another ICM user has viewed a document of theirs in the system. Using this functionality, users can "police" their records, including ROIs and Subject Records, by having notice and the ability to inquire as to why another user has conducted a particular query. Query notifications bring transparency to the system that discourages unauthorized browsing for information. If an HSI case agent suspects or has reason to believe ICM records have been misused in any fashion, the agent must report the suspected misconduct to OPR for further investigation.

Finally, ICM maintains detailed sets of auditing requirements that are tracked and saved in audit logs that can be later viewed by OPR if allegations of misuse are made against an ICM user. ICM keeps copies of audit and log file data in a separate data repository where they are retained for seven years to ensure ICE will be able to track and investigate misconduct and misuse of the system. OPR users who query ICM and the HSI Data Warehouse also have their activity tracked in the audit logs. However, their queries and viewing of ICM case records do not trigger notifications to the case agent in order to preserve the integrity and confidentiality of ongoing OPR investigations.

[46] DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), available at https://www.dhs.gov/privacy-impact-assessments.

Conclusion

Facial Recognition Technology is a rapidly developing capability that is already in use by law enforcement agencies nationally. ICE HSI's mandate to safeguard the nation and enforce immigration laws are aided exponentially through the use of third-party services that use facial recognition technology. While the technology itself does have far reaching privacy implications, HSI has established processes and procedures to mitigate the impact of an FRS on individuals. Through proper collection techniques, candidate vetting, and supervisor oversight, HSI endeavors to use FRSs in as much of a privacy sensitive manner as possible.

Responsible Officials

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

Approval Signature

[Original, signed copy on file with the DHS Privacy Office]

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment Update
for the

Student and Exchange Visitor System Admissibility Indicator

(SEVIS-AI)

DHS/ICE/PIA-001(b)
July 19, 2016

Contact Point
Peter Edge
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 Information System (SEVIS), owned and operated by U.S. Immigration and Customs Enforcement (ICE), Student and Exchange Visitor Program (SEVP), is an internet-based system that maintains real-time information on nonimmigrant students and exchange visitors, their dependents, and the approved schools and designated U.S. sponsors that host these nonimmigrants. The original Privacy Impact Assessment (PIA) for SEVIS was published on February 5, 2005. This update is to provide notice of ICE's implementation of a new method to routinely share SEVIS information with U.S. Customs and Border Protection (CBP) to assist CBP at primary inspection points with information on admissibility for nonimmigrants seeking to enter the United States in the F, M, and J classes of admission.

Introduction

U.S. Immigration and Customs Enforcement (ICE), Student and Exchange Visitor Program (SEVP) operates the Student and Exchange Visitor Information System (SEVIS) under the authority of 8 U.S.C. § 1372 in coordination with the U.S. Departments 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 collect electronically, from approved educational institutions and designated EV programs in the United States, certain information about aliens who have or are applying for F, M, or J nonimmigrant status.[2] 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 EV programs; and the alien's date and port of entry.

SEVIS 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 and spouses (F-2, M-2, and J-2 classes of admission). Designated school officials of SEVP-certified schools and responsible officers of DOS-approved programs use SEVIS to transmit mandatory information and event notifications about nonimmigrants, exchange visitors, and their dependents and spouses via the internet to DHS and DOS.[3]

---

[1] Congress mandated that DHS, in consultation with the U.S. Departments of State (DOS) and 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 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).

[3] All SEVIS data elements are described in full in the original SEVIS PIA, DHS/ICE/PIA-001 Student And

CBP officers use SEVIS information and information from the Certificates of Eligibility (Forms I-20 and DS-2019[4]) to ensure that nonimmigrants seeking admission in the F, M, or J classes of admission have a SEVIS record that supports eligibility to enter the United States. Using the SEVIS Admissibility Indicator Service (SEVIS-AI), a new web service and subsystem to SEVIS, ICE transmits select SEVIS data and admissibility indicators, determined by regulation-based business rules, [5] to CBP's Traveler Primary Arrival Client (TPAC),[6] which aggregates data on individuals from a number of systems to support admissibility decisions at primary inspection. CBP stores limited SEVIS and admissibility data in the TECS database and also makes this data available to officers at secondary inspection through the Consolidated Secondary Inspection System (CSIS).[7] 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, or J nonimmigrant; and (4) assist CBP officers in making faster, more informed decisions that greatly reduce the risk of fraudulent entry.

Reason for the PIA Update

DHS/ICE is updating the existing SEVIS PIA[8] to account for a new method for sharing select SEVIS data with CBP. Prior to this update, CBP officers at ports of entry relied on the paper-based Form I-20, Form DS-2019, and CBP's TECS[9] system when making admission decisions for the F, M, and J classes of admission. There was no direct feed from SEVIS, which has the latest information on eligibility for entry, to CBP systems. This created a risk that nonimmigrants could

---

Exchange Visitor Information System (SEVIS) (February 5. 2005), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sevis.pdf and the corresponding DHS/ICE-001 SEVIS SORN (75 FR 412, January 5, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

[4] I-20, "Certificate of Eligibility for Nonimmigrant Student Status" and DS-2019, "Certificate of Eligibility for Exchange Visitor (J-1) Status" The I-20 is used by SEVP for F-1 and M-1 nonimmigrants, while the DS-2019 is used by Department of State for J-1 nonimmigrants. These forms are not publicly available; they are provided only by designated school officials or sponsors.

[5] *See* SEVP's governing regulations for students and schools, *available at* https://www.ice.gov/sevis/schools/reg#f.

[6] TPAC is a functionality of TECS related to primary processing. *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing p. 6, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

[7] CSIS is a functionality of TECS related to secondary processing. *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing at p. 13, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf.

[8] *See supra* note 3.

[9] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf and DHS/CBP-011 TECS SORN (73 FR 77778, December 19, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.

gain entry into the United States even if their Certificate of Eligibility had been terminated, or otherwise were no longer valid. For example, an international student whose Form I-20 was terminated in SEVIS could still be admitted by CBP officers at primary inspection if the student presented a seemingly legitimate paper-based Form I-20.

Though CBP officers are authorized to access the SEVIS system directly, such access has not been practical for officers performing primary inspections who must make quick decisions to prevent long wait times, particularly at air ports of entry. Logging into SEVIS, searching for a record, and then interpreting it properly takes more time than is available for the admission decision. This update will address this issue by making SEVIS data available through TPAC, and subsequently CSIS, via SEVIS-AI.

SEVIS-AI provides CBP officers performing inspections at ports of entry rapid, real-time SEVIS data admissibility indicator, and limited biographic and program-related data (e.g., SEVIS ID, school/program name, and school/program start and end dates) to TECS. An admissibility indicator, consisting of a reason code and narrative description,[10] is generated only after SEVIS data is vetted against regulation-based business rules and the results show an issue that requires referral of the nonimmigrant to CBP secondary inspection. If after vetting there is no issue, then SEVIS-AI will not generate an admissibility indicator. As a baseline, the SEVIS-AI business rules assume all nonimmigrants are inadmissible until their SEVIS records show they meet admissibility requirements.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

There are no changes to the information collected and stored within SEVIS. ICE continues to collect the following information from nonimmigrant students, exchange visitors, and dependents: the nonimmigrant's name, country of birth, date of birth, country of citizenship, educational background, information on the education/program activity for which the nonimmigrant is seeking admittance, and passport and visa information. A list of the information collected and maintained in SEVIS on all nonimmigrant students, exchange visitors, and their dependents is in Appendix C of the 2005 SEVIS PIA and the SEVIS System of Records Notice (SORN).[11]

---

[10] Together, the reason code and narrative description identify and alert CBP officers to the reason behind the SEVIS-AI vetting result only if the result is that the nonimmigrant may be inadmissible to the United States.
[11] DHS/ICE-001 SEVIS SORN (75 FR 412, January 5, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

Existing SEVIS data is compared against automated, regulation-based business rules to determine whether admissibility indicators need to be generated in the SEVIS-AI subsystem. Admissibility indicators, along with the following data elements already collected in SEVIS, are shared through SEVIS-AI with CBP's TPAC and CSIS: SEVIS ID, nonimmigrant's name, date of birth, school/program name, and school/program start and end dates. CBP does not send any information regarding final admissions decisions or related actions back to SEVIS-AI or the primary SEVIS system.

As a web service, SEVIS-AI supports real-time responses to queries from CBP officers at primary inspection based on existing SEVIS data. SEVIS-AI does not have a user interface, but has a database instance that stores (1) SEVIS data to run the business rules and generate the admissibility indicator, (2) admissibility indicators, and (3) transactional information (e.g., date and time of response to CBP). The SEVIS-AI subsystem does not return any information to the primary SEVIS database. The admissibility indicator and transactional information is not stored in the primary SEVIS database.

SEVIS-AI also generates reports that allow ICE SEVP to view data in order to manage the business rules, measure responsiveness, and to respond to inquiries about specific cases in support of requests, such as data correction requests, Freedom of Information Act requests, congressional inquiries, or DHS Traveler Redress Inquiry Program questions.

Uses of the System and the Information

Using SEVIS-AI, ICE transmits SEVIS data and associated admissibility indicators to CBP officers at ports of entry to streamline the admissions process and inform admissions decisions for nonimmigrants seeking to enter the United States in the F, M, or J classes of admissions.

SEVIS-AI sends a request to the primary SEVIS system for new or updated SEVIS records.

SEVIS-AI receives a daily feed of SEVIS records that have been added or updated since the last feed. It runs a set of business rules against each record to determine whether a nonimmigrant meets the criteria for admissibility in the F/M/J class of admission. When SEVIS records support a decision to admit, no admissibility indicator is generated. 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 query from an officer at primary inspection using TPAC.

When a nonimmigrant seeks admission at a port of entry, a CBP officer selects the class of admission (i.e., F, M, or J) in CBP's TPAC system and enters the nonimmigrant's SEVIS ID.[12] Using the SEVIS ID, TPAC queries SEVIS-AI, and SEVIS-AI sends a response back to TPAC that includes select SEVIS data and the admissibility indicator, if there is one. For example, an admissibility indicator may indicate that a nonimmigrant has a terminated SEVIS record or is attempting to enter the United States prior to his or her authorized date of entry.

CBP officers at primary inspection view SEVIS data and admissibility indicators only in TPAC. Most nonimmigrants with admissibility indicators are referred for secondary inspection. Officers in secondary have additional time to determine if there is mitigating information. Similar to officers in primary using TPAC, officers in secondary use CSIS to access the same SEVIS data and admissibility indicators, but they can also log directly into SEVIS to access full SEVIS records to make final entry decisions.

SEVIS-AI does not contain a user interface, thereby eliminating the risk that ICE or CBP personnel may alter the admissibility indicators for F/M/J nonimmigrants attempting to enter the United States. In addition, all SEVIS-AI transmissions are logged and auditable, and include the CBP ID for the officer who initiated the query from TPAC. Lastly, though CBP officers in secondary inspection may access – in addition to the data included with the SEVIS-AI transmission – additional SEVIS data directly in the primary system, ICE granted these CBP users access to SEVIS prior to implementation of the SEVIS-AI process.

SEVIS-AI Business Rules

The basis for the SEVIS-AI business rules are the existing regulations governing F, M, and J status and admissibility.[13] These rules help ensure consistent application of the regulations. As a baseline, the SEVIS-AI rules assume all nonimmigrants are inadmissible until their SEVIS records show they meet admissibility requirements.

The SEVIS-AI subsystem has the capability for SEVP to make some modifications to the business rules. Rules can be updated to change: the requirement for fee payment; the length of time an F, M, or J nonimmigrant is admissible before and after the program start date; and the length of time an F-1 or M-1 nonimmigrant is admissible after his or her program or employment ends (i.e. to add or delete a grace period).

Privacy Risk: There is a risk that the business rules, when run against the SEVIS data each day, may incorrectly identify a nonimmigrant as eligible or ineligible to enter the United States or

[12] CBP officers may access SEVIS IDs through an existing interface between TPAC and the Department of State's Nonimmigrant Visa system or from the Certificates of Eligibility forms (Forms I-20 and DS 2019).
[13] *See* 8 CFR Part 214.2.

that the nonimmigrant's eligibility status may change from the time the business rules were applied to the SEVIS data and the nonimmigrant attempts to enter the country.

Mitigation: SEVIS-AI is configured so that the business rules are run in real-time, meaning that when CBP officers query TPAC to determine a nonimmigrant's eligibility status, the business rules are re-applied to the SEVIS data at the time of the query, and the resultant admissibility indicator is transmitted from through SEVIS-AI to TPAC. This re-application of business rules is further explained in the Technology section of this PIA Update.

Privacy Risk: There is a risk that the business rules may be modified inappropriately.

Mitigation: SEVP established an oversight process for requesting changes to business rules. Business rules are based on regulations. Only new regulations would result in new business rules. Business rules may be changed in SEVIS-AI only at SEVP's request, and require approval by the system owner. Once approved, the planned change goes through the change control process, which includes documenting the details of and reason behind the change and culminates in the change being implemented by the system developer.

Retention

There is no change to the retention of SEVIS data. The SEVIS records schedule will apply, which call for retention of the data for 75 years. The retention of SEVIS and admissibility indicator data accessed and viewed by CBP in TPAC and CSIS and stored in TECS will be addressed in CBP's Privacy Impact Assessment related to the TECS Platform.

Internal Sharing and Disclosure

As described above, ICE is implementing a new method for sharing SEVIS data and admissibility indicators with CBP. CBP officers at ports of entry use this data to inform their admissions decisions for nonimmigrants seeking to enter the United States in the F, M, or J classes of admissions. CBP officers at primary inspection access select SEVIS data (e.g., SEVIS ID, nonimmigrant's name, date of birth, school/program name, and school/program start and end dates) and admissibility indicators, if present, through TPAC, which aggregates data on individuals from a number of systems to support admissibility decisions. CBP stores the SEVIS ID and admissibility indicator, including reason code and description, in the TECS database. If a nonimmigrant is referred to secondary inspection, CBP officers will access the data through CSIS, to better understand why the nonimmigrant was referred.

Privacy Risk: There is a risk that CBP officers will use admissibility indicators to refuse entry without conducting the appropriate investigations.

Mitigation: CBP officers at primary inspection use admissibility indicators only as the basis for referring a nonimmigrant to secondary inspection. At secondary inspection, a separate CBP officer will make a final determination regarding admissibility after reviewing any referred admissibility indicators and all other relevant information concerning the indicators and the nonimmigrant. The purpose of the admissibility indicator at primary inspection is to alert the CBP officer to refer the nonimmigrant to secondary inspection for the admissions decisions.

Privacy Risk: There is a risk that SEVIS information will be improperly disseminated to the TECS users, outside the scope of the SEVIS SORN.

Mitigation: The information from SEVIS-AI that is captured and saved into TECS is limited to the SEVIS ID and admissibility indicator. Other information, such as name and date of birth, are already captured in other systems that use the TECS platform for data storage. Information on the TECS platform is limited to need to know access and have security controls in place to protect sensitive information. A new TECS user must also complete the TECS Security and Privacy Awareness course and pass the associated test before CBP grants initial TECS access. The course presents Privacy Act responsibilities and Agency policy regarding security, sharing, and safeguarding of official information and PII on the TECS Platform. The course also provides a number of sharing and access scenarios to test the prospective user's understanding of appropriate controls put in place to protect privacy. This training is regularly updated and TECS users are required to take the course annually.

External Sharing and Disclosure

External sharing and disclosure of SEVIS data will not change with this update.

Notice

There are no changes to the notice required or provided to individuals whose information may be maintained in the SEVIS database or shared via the SEVIS-AI service. General notice about the information maintained in the system and how it is shared is provided by the DHS/ICE/PIA-001 SEVIS PIA (February 5, 2005), this update, and the DHS/ICE-001 SEVIS System of Records Notice (SORN).[14]

[14] DHS/ICE-001 SEVIS SORN (75 FR 412, January 5, 2010), *available at* https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

Individual Access, Redress, and Correction

This PIA update does not change the ability of an individual to request access, redress, and correction of his or her information. As the primary SEVIS database is the source of information for the SEVIS-AI, there is no need to change in the existing methods for redress and correction.

Additionally, SEVP can quickly update the business rules in SEVIS-AI subsystem if experience shows that a particular business rule causes a misinterpretation of the regulations and thus generates an incorrect admissibility indication.

Technical Access and Security

As the SEVIS-AI subsystem does not have a user interface, there is no direct user access to SEVIS-AI. A database instance of SEVIS-AI stores the select SEVIS data and admissibility indicators passed to CBP, including the date and time of the transactions; the location of the workstation that received the information; and the CBP requestor's ID. This information is not returned to the primary SEVIS database. Select SEVP users have access to this stored data for the purpose of managing and auditing SEVIS-AI.

All ICE and CBP users who have access to SEVIS, SEVIS-AI, TPAC, and CSIS are required to complete annual privacy and security training.

Technology

SEVIS-AI changes the technology ICE uses to share SEVIS information with CBP. Since SEVIS-AI is a subsystem of SEVIS, it is covered by the SEVIS Authority to Operate (ATO). The SEVIS ATO was granted on July 18, 2013, and will expire on July 18, 2016.

Each day, SEVIS-AI sends a request to the primary SEVIS system for new or updated SEVIS records. Upon receipt of these records from SEVIS, SEVIS-AI applies the business rules to each SEVIS ID to determine whether an admissibility indicator needs to be generated. When CBP officers at primary inspection points use TPAC to process a nonimmigrant seeking entry in an F, M, or J class of admission, TPAC sends a request via a secure Internet connection to SEVIS-AI. SEVIS-AI finds the record, re-applies the business rules, and sends the response via the secure Internet connection where it is displayed to the CBP officer in TPAC.

SEVIS-AI reapplies the business rules when responding to a CBP query because many of the business rules are based on the relationship between the date of entry and a date on the SEVIS record. For example, SEVIS may send a new record to the SEVIS-AI subsystem for a J-1 nonimmigrant with a SEVIS record status of "Initial." On the day the record is sent to the SEVIS-AI subsystem, an admissibility indicator would display if the nonimmigrant's program start date is more than 30 days in the future. However, when the nonimmigrant appears at the port of entry,

the program start date might be less than 30 days in the future, so after recalculation, no admissibility indicator would display by SEVIS-AI. TECS ingests the SEVIS ID as part of the I-94 form completed via TPAC and CSIS, and the admissibility indicator reason code and description as part of the TECS audit log.

Responsible Official

Amber Smith
Privacy Officer
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

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 **U.S. Department of Homeland Security Form I-901,** "Fee Remittance Form for Certain F, J and M Nonimmigrants," OMB Control No. 1653-0034 **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 **U.S. Department of Homeland Security Form I-765**, "Application for Employment Authorization," OMB Control No. 1615-0040 **U.S. Department of Homeland Security Form I-539**, "Application to Extend/Change Nonimmigrant Status," OMB Control No. 1615-0003 **U.S. Department of Homeland Security Form I-94**, "Arrival/Departure Record," OMB Control No. 1651-0111 **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 **U.S. Department of State Form DS-7002, "**Training/Internship Placement Plan," OMB Control No. 1405-0170 **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 **U.S. Department of Homeland Security Form I-765**, "Application for Employment Authorization," OMB Control No. 1615-0040 **U.S. Department of Homeland Security Form I-539**, "Application to Extend/Change Nonimmigrant Status," OMB Control No. 1615-0003 **U.S. Department of Homeland Security Form I-94**, "Arrival/Departure Record," OMB Control No. 1651-0111 **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 **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
- Determination and Status
- Compliance

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
- Identity Verification
- Auditing
- 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.