Privacy Impact Assessment
for the

Visa Security Program - Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) Tracking System

DHS/ICE/PIA-052

March 10, 2020

Contact Point
Alysa Erichs
Acting Executive Associate Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement

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

Abstract

The Visa Security Program - Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) is a U.S. Immigration and Customs Enforcement (ICE) tracking system designed to support the activities of the ICE Homeland Security Investigations (HSI) Visa Security Program (VSP). ICE originally deployed VSP-PATRIOT in 2014, and it is operated by the Visa Security Coordination Center (VSCC), the primary national security and counterterrorism planning component for ICE, in partnership with the U.S. Customs and Border Protection (CBP) and the U.S. Department of State (DOS). VSP-PATRIOT allows authorized personnel from ICE, CBP, and DOS to identify applicants for U.S. visas who are ineligible to receive visas and inadmissible to the United States due to criminal history, terrorism-related associations or activity, other security-related offenses, or any other grounds of ineligibility or inadmissibility. ICE is conducting this Privacy Impact Assessment (PIA) in the interest of transparency as the VSP-PATRIOT tracking system automates the system-to-system connections memorialized in the existing VSPTS-Net PIA.[1] In addition, this PIA provides insight into the supplemental review of publicly available, open-source information performed with respect to a small subset of applicants.

Overview

ICE established the VSP in support of Section 428 of the Homeland Security Act of 2002, 6 U.S.C. § 236. Following its inception, ICE developed the VSP-PATRIOT tracking system to support the visa security work performed by HSI Special Agents at U.S. embassies and consulates ("consular posts"). VSP-PATRIOT manages the workflow associated with the screening and vetting[2] of all non-immigrant visa applications by HSI and CBP personnel[3] prior to DOS adjudication and allows personnel overseas to leverage the VSP investigative capabilities to conduct interviews, coordinate with federal agencies and foreign counterparts, and review any derogatory information.[4] VSP-PATRIOT interfaces with the DOS Consular Electronic

[1] *See* DHS/ICE/PIA-011 Visa Security Program Tracking System (VSPTS-Net) and subsequent update, *available at* https://www.dhs.gov/privacy.
[2] For purposes of this PIA, "screening and vetting" is defined as manual and automated processes used to identify and analyze information in U.S. Government holdings to determine whether an individual poses a threat to national security, border security, homeland security, or public safety, primarily, but not necessarily exclusively, in support of the U.S. Government's visa, naturalization, immigration benefit, immigration enforcement, travel, and border security decisions about an individual.
[3] In this context, "HSI and CBP personnel" may be either federal employees or contractors performing screening and vetting activities in the National Capital Region (NCR).
[4] Derogatory information is information about individuals that may include, but is not limited to, criminal or terrorist information or activities, or other information related to an on-going or potential investigation or law enforcement operations.

Application Center (CEAC)[5] and Consular Consolidated Database (CCD)[6] systems via the CBP Automated Targeting System (ATS)[7] to document investigative information found during the application and interview ("case") screening and vetting phases.

After reviewing and vetting applications, HSI Special Agents at consular posts provide DOS, via the VSP-PATRIOT system, with recommendations regarding the applicants' eligibility for visas, a summary of relevant notes, the application's request identifiers, and the relevant code(s) of law if the Department of Homeland Security (DHS) is recommending that a visa application be refused.[8] Authorized DOS personnel, including DOS Assistant Regional Security Officers for Investigations (ARSO-Is), access CCD to view DHS's recommendation based on the investigative information found related to the vetting of visa applicants. DOS personnel can search for specific visa applicants, view summary information from an application, view an applicant's screening results from searches made against DHS derogatory information assets, and view and add attributes and notes to memorialize the results of any pertinent DOS investigations conducted while vetting the applicant. Any individual identified as requiring further investigation will be flagged by DHS through the ATS Unified Passenger (ATS-UPAX)[9] hotlist as being under review and may not be issued a visa until DHS provides a final recommendation.

Visa Screening and Vetting Process: Application and Interview (Case) Phases

During the visa application screening and vetting phase, the visa applicant completes his or her visa application via the CEAC system and the application is passed to CCD through an automatic system-to-system interface. The CEAC visa application contains information pertaining to both the visa applicant him/herself, as well as individuals associated with the applicant. Regarding the applicant, the visa application lists biographical, employment, and contact information. The CEAC application also contains contact information about the applicant's associates, as DOS may consider associate information when determining whether to grant or deny a visa. The application is then sent to ATS to be screened against derogatory information and targeting rules.[10] Subsequently, as a part of the standard visa issuance process, visa applicants are

---

[5] *See* the DOS CEAC PIA (April 2018), *available at* https://2009-2017.state.gov/documents/organization/242319.pdf.

[6] CCD is the official repository of visa records from U.S. consular posts around the world. For additional information, s*ee* the DOS CCD PIA (July 2015), *available at* https://2009-2017.state.gov/documents/organization/242316.pdf.

[7] *See* DHS/CBP/PIA-006(e) Automated Targeting System, *available at* https://www.dhs.gov/privacy.

[8] For each application, the role of HSI and CBP personnel is limited to providing DOS with a recommendation of whether to issue a visa.

[9] *See* DHS/CBP-006 ATS PIA, *available* at www.dhs.gov/privacy. UPAX is an interface that provides direct access to information from partner agency databases and produces query results across multiple source systems.

[10] Targeting rules are criteria developed by DHS from trend analysis, law enforcement cases, and intelligence used for screening purposes. For a complete assessment of the rules process and procedures within ATS, please see the 2012 PIA for ATS: DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update, *available at* https://www.dhs.gov/privacy.

required to appear at the visa issuing consular post for an interview with a DOS official. When the visa applicant comes to the consulate for the required interview, the visa application is classified as a "case" and a DOS official verifies and updates, as needed, the information previously submitted in the visa application. CCD sends the updated visa application information to ATS, which again screens the applicant against the derogatory information and targeting rules in ATS, independent of the results from the screening and vetting conducted in the application phase. ATS then sends the updated application and ATS interview (hereafter "case") phase screening results to VSP-PATRIOT. VSP-PATRIOT displays results from both the application phase and the case phase with corresponding hits to be reviewed by the DOS official for consideration prior to issuing the visa.

Screening and Vetting Results

If there is a match to any derogatory information for the visa applicant, the ATS screening results sent to VSP-PATRIOT show the name of the system that was the source of the derogatory information about the applicant (i.e., ATS) and the data element(s) for which there was a match (e.g., the applicant's name, date of birth, passport number). The actual content of the data element for which there was a match is not sent automatically to VSP-PATRIOT.[11] If there is a match to targeting rules, the screening results provide an identifier for the targeting rule and a brief explanation of the rule, such as "terrorism activity." VSP-PATRIOT then flags those applications for review by analysts in the NCR and HSI Special Agents, who will determine whether there is criminal history or terrorism-related information, a record of immigration violations, or other information relevant to the applicant's eligibility for a visa and evaluate the need for and carry out further investigation (e.g., liaise with local law enforcement officials). The HSI Special Agents record information related to their reviews and recommendations in the notes section of VSP-PATRIOT. VSP-PATRIOT sends the DHS visa recommendation to CCD with details related to each hit. Using the information provided to CCD, DOS officials then make the final decision on visa issuance.

If there are no matches against derogatory information or targeting rules for the applicant, ATS sends VSP-PATRIOT an indication that there are no matches. In the application phase, the indication is a "Green Screen Result." In the case phase, the indication that there are no matches states "Green Screen Result of No Objection without Comment." Both such indications inform the DOS official that it is clear to issue the visa without further input from DHS.

Public-Facing, Open-Source Information

At certain consular posts as part of a pilot program, HSI Special Agents conduct supplementary screening and vetting of visa applications using publicly available, open-source

[11] For example, ATS will indicate that a match was found as a result of the applicant's name, but the actual name will not be automatically sent to VSP-PATRIOT.

information. The VSP receives a daily email of CEAC data consisting of applications submitted to the five consular posts participating in the pilot program. HSI Special Agents leverage a third-party commercial tool ("tool")[12] to conduct Internet searches using commercial databases that provide aggregated publicly available information obtained from social media and other Internet sites for potential derogatory or high-risk information associated with visa applicants.

During this process, HSI Special Agents manually upload the CEAC data received into the tool, which then analyzes a subset of the visa application data elements. The data elements may include biographical, employment, and contact information about the visa applicant.[13] Information pertaining to the applicant's associates (as listed on the visa application) is not uploaded into the tool. The tool searches against public-facing websites to determine individuals who are suspected of, associated with, or engaged in criminal or terrorism-related activities, and provides a score indicating the confidence that the information is associated with the relevant visa applicant.[14] HSI Special Agents look at the highest scored matches and determine which ones to vet manually. HSI uses manually vetted public-facing information as supplementary data to government holdings to determine those individuals who require further investigation. HSI Special Agents may choose, at their discretion, to document the information found from using the tool in the visa applicant's file in VSP-PATRIOT. Any determination of risk obtained from the use of the tool does not, on its own, result in a negative recommendation.

Recording DOS Final Determinations

After DOS makes its final decision and either issues or refuses the visa, the final determination is recorded in CCD, which updates the CBP TECS system (not an acronym) with DOS' final determination. TECS is an information-sharing platform used by law enforcement officials to assist with screening and determinations regarding the admissibility of arriving persons.[15] TECS shares this final determination with ATS. TECS may also share the final determination with ICE's Investigative Case Management (ICM) system[16] for the creation or modification of a case file.

---

[12] The third-party commercial tool is used to search publicly available information from open sources and social media sites belonging to subjects of investigations. HSI Special Agents access the tool through the vendor's web portal. For additional information on the tool, see the DHS/ICE/PIA-044 LeadTrac System PIA, at https://www.dhs.gov/privacy.

[13] VSP-PATRIOT is not directly associated or interfaced with the third-party commercial tool but leverages its vetting function for screening visa applicants.

[14] The score is generated through an algorithm built into the third-party tool. The tool leverages domain-specific indexes of the internet using a sophisticated risk-scoring method that targets specific information.

[15] *See* DHS/CBP/PIA-009(a)-TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative, *available at* https://www.dhs.gov/privacy.

[16] *See* DHS/ICE/PIA-045 ICE Investigative Case Management (ICM), *available at* https://www.dhs.gov/privacy. The actual derogatory information is highlighted in ICM in the form of a Report of Investigation (ROI).

VSP-PATRIOT enables users to generate ad-hoc reports in support of the VSP. These reports typically provide metrics on the activities performed by agents, officers, and analysts such as the number of application records screened on a given day or for a particular part of the world, the average number of days to process applications, and the number of applications in which there was a conflict between the DHS recommendation and DOS decision.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

HSI operates VSP-PATRIOT pursuant to Section 428 of the Homeland Security Act of 2002,[17] and 22 C.F.R. § 41.121, which permit the refusal of visas if the Secretary of State deems a refusal "necessary or advisable in the foreign policy or security interests of the United States." VSP-PATRIOT allows HSI and CBP personnel to identify those applicants for U.S. visas who are inadmissible to the United States due to criminal history, terrorism associations, or other security-related grounds, and provides the DOS with the requisite information for making visa eligibility determinations.

In addition, VSP-PATRIOT is supported by the following interagency agreements:

- The Memorandum of Understanding (MOU) between the Secretaries of State and Homeland Security concerning the implementation of Section 428 of the Homeland Security Act of 2002, signed on September 26, 2003, which governs the implementation of Section 428 by these agencies.
- The Memorandum of Agreement (MOA) between DOS and the DHS regarding the sharing of visa, passport records, and immigration, naturalization, and citizenship records (hereafter, DOS-DHS MOA), signed on November 18, 2008.
- The MOU between the DOS Bureau of Consular Affairs and the DHS/ICE for Cooperation in Data Sharing (Visa and Immigration Data), signed on October 6, 2006, which is incorporated into the DOS-DHS MOA.

The disclosure and sharing of visa record information by the DOS with DHS is subject to confidentiality requirements under Section 222(f) of the Immigration and Nationality Act (INA).[18]

[17] *See* Homeland Security Act of 2002 § 428(e), 6 U.S.C. § 236(e) (discussing the assignment of DHS employees to diplomatic and consular posts).
[18] *See* 8 U.S.C. § 1202(f).

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The DHS/ICE-012 Visa Security Program Records SORN applies to the information implicated by VSP-PATRIOT.[19]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes; the most recent version of the Security Plan (SP) in support of VSP-PATRIOT was approved on May 16, 2016.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes; the records retention schedule, N1-567-10-005, was approved by NARA in February 2010.[20]

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

HSI and CBP personnel do not perform "collections of information" from the public in support of VSP-PATRIOT; therefore, this activity is not covered by the PRA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The VSP-PATRIOT tracking system ingests only the required information pertaining to visa applicants from ATS. DOS's CCD system automatically sends the CEAC application to ATS, and in accordance with ATS's targeting rules established for visa vetting, ATS conducts a check for derogatory information related to the visa applicant. ATS then sends the screening results to VSP-PATRIOT, which will indicate a match or no match. VSP-PATRIOT maintains the final

[19] *See* DHS/ICE-012 Visa Security Program (VSP), 74 FR 50228 (Sept. 30, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.
[20] *See* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0567/n1-567-10-005_sf115.pdf.

DHS recommendation, relevant code(s) of law if DHS is recommending that the visa application be denied, and the final adjudication decision made by DOS.

VSP-PATRIOT Subject Information Section:

While ATS itself stores the individual's complete application and thus, the information contained within a visa application (e.g., Social Security number [SSN], Alien Registration Number [A-Number], U.S. Driver's License Number, and U.S. Taxpayer ID), only the information that is compatible with the purpose of VSP-PATRIOT is maintained in the tracking system.[21] The only information displayed in the applicant's visa case subject information section in the VSP-PATRIOT application is:

- Name
- Alias
- Nationality
- DOB
- Gender
- Country of birth
- Record type
- CCD system key
- Visa type
- Record type
- Document number
- DOS-issued bar code
- Visa case request ID number
- Visa post

VSP-PATRIOT Adjudication Information Section

In addition to the summary information section, HSI and CBP personnel may include additional information in a free text field of the applicant's visa case file called the adjudication information section. This section may document limited information from the applicant's CEAC

[21] During the ingestion of the visa application information from ATS, VSP- PATRIOT performs a system check to ensure that those data elements are not ingested into the system.

application that has been compiled by HSI and CBP personnel while reviewing and vetting the applicant. The data collected by DOS on the CEAC application includes, but is not limited to:

- Biographic information about the applicant including name, address, phone number, email address, date of birth, country of birth, and nationality;
- Contact information (i.e., name, phone number, email address, address) about other individuals associated with the visa applicant, including the applicant's spouse, individuals traveling with the applicant, the application preparer's name, and the applicant's point of contact in the United States/U.S. sponsor/petitioner, if any;
- Travel information, including information regarding past trips to the United States;
- Identification numbers, including passport number, passport book number, non-U.S. national ID, and Student and Exchange Visitor Information System (SEVIS) ID;
- Name and address of employer and/or school;
- The type of visa for which the applicant is applying;
- Security and background-related information,[22] including:
    - Medical and health information (for example, questions about communicable diseases the applicant may have);
    - Criminal history information (for example, previous convictions);
    - Security-related information (for example, questions about the applicant's past history and/or intention to engage in espionage or terrorist activities); and
    - Immigration-related information (for example, previous deportations, removals, or overstays).

As discussed above, HSI Special Agents at select locations manually upload data contained in the CEAC applications into a tool that searches public-facing, open source information, including social media, for potential derogatory or high-risk information pertaining to visa applicants. The CEAC data elements uploaded to the tool may include biographical, employment, and contact information about the visa applicant, as bulleted above. The information provided by the visa applicant is considered a visa record subject to the confidentiality provisions of section 222(f) of the INA. HSI Special Agents may choose, at their discretion, to document the information found from using the tool in the visa applicant's case under the adjudication information section in VSP-PATRIOT.

[22] These questions are true/false questions and the applicant provides descriptions related to any affirmative answers.

Finally, VSP-PATRIOT maintains name and business contact information about the agents, officers, and analysts that log into the system to perform administrative duties and conduct the visa security reviews. It also enables users to generate reports in support of the VSP. These reports typically provide metrics on the activities performed by agents, officers, and analysts such as the number of applications records screened on a given day or for a particular part of the world, the average number of days to process applications, and the number of applications in which there was a conflict between the DHS recommendation and DOS decision. These reports do not contain PII.

2.2 What are the sources of the information and how is the information collected for the project?

Visa application data is obtained by DOS from the individual visa applicant via CEAC and ingested into the CCD system. CCD sends the data to ATS for screening. ATS then sends the screening results for possible matches to derogatory information and/or targeting rules to VSP-PATRIOT. HSI and CBP personnel may also obtain information through queries of other federal databases including but not limited to CBP's Arrival Departure Information System (ADIS),[23] ICE's Student and Exchange Visitor Information System (SEVIS),[24] and ICE's Enforcement Integrated Database (EID).[25] Agents, officers, and analysts may also obtain information from other sources during the review including from foreign governments, Interpol, Europol, employers, public records, family members, and other individuals and entities who may be interviewed or serve as sources of information in order to determine or confirm an applicant's identity or to verify information provided by the visa applicant.

HSI may also obtain information from open-source sites including from social media sites and commercial data aggregators during their reviews. HSI may conduct Internet searches for birth records, death records, real estate records, address information, and other government-issued identification records. The information is used to determine or confirm an applicant's identity or to verify information provided by the visa applicant. HSI may choose to document the information found on public websites in the visa applicant's file in VSP-PATRIOT.

All transmission of data between CEAC, CCD, ATS, and VSP-PATRIOT occurs via secure electronic system-to-system connections.

[23] *See* DHS/CBP/PIA-024(b) Arrival and Departure Information System (ADIS), *available at* https://www.dhs.gov/privacy.
[24] *See* DHS/ICE/PIA-001(c) Student and Exchange Visitor Information System (SEVIS), *available at* https://www.dhs.gov/privacy.
[25] *See* DHS/ICE/PIA-015(j) Enforcement Integrated Database (EID) EAGLE, EDDIE, and DAVID, *available at* https://www.dhs.gov/privacy.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

At select locations, HSI provides a subset of visa application data elements to a third-party commercial tool to search public-facing, open source information, including social media sites, for potential derogatory or high-risk information pertaining to visa applicants. The tool uses the data to search against domain-specific public-facing open source information, including social media, and determines individuals who are suspected of, associated with, or engaged in criminal or terrorism-related activities as well as a score indicating the confidence that the information is associated with the relevant visa applicant. Any determination of risk from the Internet searches does not, on its own, result in a negative recommendation. However, the results documented in VSP-PATRIOT supplement data in government holdings to determine those individuals that require further investigation.

2.4 Discuss how accuracy of the data is ensured.

There are several aspects of the program that help to ensure data accuracy. First, DOS collects information directly from the visa applicant through the visa application. During the visa interview process, known as the case phase of the application process, DOS collects information directly from the applicant related to the visa application, including biographical information, at which time the information is deemed to be highly accurate since the individual has control of the information being self-reported. Second, the automated system-to-system interfaces among CEAC, CCD, ATS, and VSP-PATRIOT help to ensure data accuracy because users are not manually querying and/or entering data into each system. Instead, information is shared directly among the systems. Finally, the additional checks and manual vetting performed by HSI and CBP screening and vetting analysts against federal databases and publicly available websites help to identify and correct potential inconsistencies or inaccuracies in the data. All these factors contribute to greater data accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that HSI will receive more information about visa applicants and/or their associates than is necessary to accomplish the purposes of the VSP.

Mitigation: The information collected about visa applicants and their associates on the CEAC form by DOS is used to determine the eligibility of foreign nationals who apply for a U.S. visa. The information provided by the visa applicant is considered a visa record subject to the confidentiality provisions of section 222(f) of the INA. Only information relevant to determining the eligibility of the applicant and related to DHS's reviews and recommendations is added to

VSP-PATRIOT.[26] Any SSNs, A-Numbers, Driver's License Numbers, or U.S. Taxpayer IDs that may accompany applications are not ingested into VSP-PATRIOT from ATS. The information that VSP-PATRIOT collects is necessary for documenting investigative information to be used in vetting visa applicants. The public-facing, open-source information about visa applicants from the select sites documented in VSP-PATRIOT is used to supplement data in government holdings to determine those individuals that require further investigation.

Privacy Risk: There is a privacy risk that incorrect information could be attributed to a visa applicant.

Mitigation: Several checks are in place to ensure that incorrect information is not attributed to a visa applicant. First, DOS collects information directly from the visa applicant, and information checks are performed against government data systems to ensure accuracy. Second, any indicators of risk obtained from the scoring by the third-party tool to indicate reliability are manually investigated before any further action is taken. Third, HSI reviews the information collected about visa applicants and others during the visa security review before a final decision is made on an application. Fourth, HSI checks information in visa applications against various federal databases and other sources. Collecting and comparing information from a variety of sources, including the visa applicant himself or herself during the visa security review helps ensure that information is attributed to the appropriate individual, and if incorrect information is identified, HSI can correct it before DOS makes a final determination on the visa application. Fifth, the VSP-PATRIOT program works closely with the National Counterterrorism Center (NCTC) and the Terrorist Screening Center (TSC) to ensure the accuracy of records attributed to an applicant based on National Unique Identifier Number (NUIN) hits.[27] Sixth, HSI Special Agents participate with DOS in the visa interview process to resolve any questions that cannot be matched or definitively solved through database record searches. Finally, VSP-PATRIOT analysts have access to DOS, DOJ, Interpol, Europol, public records, foreign governments, and other sources to ensure the accuracy of DOS applicant hits against ATS.

[26] The CEAC visa record sent to ATS to be screened, includes the applicant's information and contact information about other individuals associated with the visa applicant. If DHS finds derogatory information about either the visa applicant or his/her associates, then DHS will note the existence of derogatory information in VSP- PATRIOT as part of its recommendation to grant or deny the visa. The substance of the derogatory information (e.g., individual is affiliated with a gang or known terrorist organization) will be highlighted in ICM in the form of an ROI.
[27] NUIN is a unique identifier used by the FBI for individuals suspected of terrorism.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DHS uses this information to screen U.S. visa applicants for security concerns, determine who requires further scrutiny before a visa eligibility determination is made, and make a recommendation to DOS regarding the visa applicant's eligibility for a visa. HSI and CBP personnel review visa applicants to determine if individuals are ineligible to enter the United States due to criminal history, terrorism associations, or other security-related grounds. The results of the reviews are recorded in VSP-PATRIOT, including any information HSI conveys to DOS and CBP. DOS officials use the information as part of their process in deciding whether to refuse or approve applicants' visas. CBP officials use the information in two ways: (1) To keep track of the applications that possibly match derogatory information and/or targeting rules and thus need to be more thoroughly reviewed by the HSI Special Agents at the consular posts; and (2) To enhance the screening criteria used by ATS. For example, CBP uses the information provided to identify trends that can finely tune algorithms for establishing and/or modifying targeting rules. The information is also used to manage and prioritize the work of HSI personnel assigned to the VSP. Once visa applications have been screened against ATS, applications that possibly match derogatory information and/or targeting rules are flagged to be more thoroughly reviewed by HSI Special Agents. Applications that have been flagged are prioritized in VSP-PATRIOT by the type of match so that high priority applications such as terrorist-related matches are reviewed first. The aggregate information in the system and the metrics developed about the VSP are shared with other VSP offices at locations abroad and with ICE headquarters to facilitate visa security reviews and oversight of the program. When handling information about a known or suspected terrorist, HSI will work with the ICE Watchlisting Cell to ensure appropriate adjudications and the maintenance of accurate information.[28]

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. VSP-PATRIOT is a visa security program tracking system used to document information found during the visa security review process.

[28] ICE stood up a Watchlisting Cell in March 2016 that was incorporated as part of the VSP-PATRIOT Program and provides the screening and vetting for the Visa Security Coordination Center. The ICE Watchlisting Cell uses a unique Watchlisting system, which ensures appropriate DHS information is made available to NCTC and TSC on known or suspected terrorists, consistent with Federal Watchlisting guidance. ICE also uses the Watchlisting Cell data for investigations, law enforcement screening support, student exchange visitor information, and intelligence coordination.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. VSP-PATRIOT is used by both HSI and CBP personnel as the tracking tool for the DHS visa vetting security process. HSI personnel assigned to support the VSP have the permissions needed to review visa applications and to provide feedback and recommendations (refusal, revocation, no objection) to DOS. ARSO-Is and Foreign Service Nationals (FSNs)[29] may also have limited role-based access to the system.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of misuse by authorized users, including making unauthorized disclosures of the information in the system.

Mitigation: In the standard operating procedures for VSP-PATRIOT and in the specialized training provided to system users, individuals are instructed how to properly protect information in the system from inappropriate disclosure to third parties. In addition, all personnel must take annual computer security and privacy training. Individuals who are found to have accessed or used the VSP-PATRIOT data in an unauthorized manner will be disciplined appropriately. In addition, HSI conducts regular audits of VSP-PATRIOT users and their use of the system and maintains an audit trail of activity in the system.

Privacy Risk: There is a risk of unauthorized access to the system.

Mitigation: The risk that VSP-PATRIOT information will be accessed in an unauthorized manner is mitigated by the fact that only individuals that have a need-to-know the information in the performance of their official duties have access to the system. Each user receives an individual account, and group accounts are not allowed. Additionally, users take annual security and privacy training and all users receive training on how to properly use the system. Finally, HSI conducts regular self-audits of users and maintains an audit trail of activity in the system in accordance with DHS 4300A Sensitive Systems Handbook.[30]

[29] FSNs are ICE staff members who hold foreign citizenship or dual citizenship with the United States and another country. FSNs fill roles that ultimately assist ICE with its mission. FSNs work at overseas ICE Attaché offices and as Task Force Officers assisting ICE overseas. FSNs do not have the authority to recommend approval or disapproval to the DOS but assist with fulfilling programmatic, administrative, investigate ve, and host country tasks as assigned.
[30] For more information, *see* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

DOS collects the information in the visa application directly from the visa applicant thus making the individual aware of the information that is being collected. Notice is provided on the CEAC form regarding the type of information to be collected, justification for the collection, routine uses, potential sharing arrangements, data protection measures, and the consequences of not providing information. Additionally, the DHS/ICE-012 Visa Security Program Records SORN and this PIA along with the DOS/STATE-39 Visa Records SORN[31] and the CEAC PIA provide notice to individuals regarding the collection, intended use, and sharing of this information.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Application for a U.S. visa is a voluntary action. Individuals who voluntarily apply for a U.S. visa are asked to supply the requested information. As indicated on the CEAC form and reiterated by the DOS official (who is the final adjudicator) a visa applicant may decline to provide information; however, he or she is advised that not providing the information may result in a delay or refusal of visa services because the United States does not have all the information it needs to effectively vet the person and make a determination about his or her visa application. Visa applicants who provide information in their visa application have no right to consent to particular uses of the information or to limit how the information is used. It is the responsibility of DOS to convey the uses of the visa applicant's information when the information is collected. The CEAC form at the time of data collection contains a Privacy Statement, which indicates what information is collected, why, for what purpose the information will be routinely used, with whom the information will be shared, and the consequences of not providing the data requested.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that applicants or their associates may not receive adequate notification about the collection and uses of their information.

Mitigation: DOS collects the information in the visa application directly from the visa applicant and notifies the individual of the purpose for the information collection, how the information will be used, and potential outcome of not providing information through the Privacy

[31] For more information, *see* https://2009-2017.state.gov/documents/organization/242619.pdf.

Act Statement displayed on the CEAC form.[32] Applicants, and any associates listed on the individual's application also receive notice through the CEAC PIA, this PIA, and the VSP Records SORN on the information that is collected and on how the information is used and shared as part of the visa application process. Additionally, the CEAC website displays a disclaimer which informs the applicant of DOS' privacy policy regarding the nature, purpose, use and sharing of PII.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

There are multiple categories of records retained in VSP-PATRIOT with varying retention periods, depending on the type of recommendation issued by HSI.

(1) Records of visa security reviews will be retained for 25 years after the date of review for records which (a) HSI does not object to the issuance of a visa because there were no matches against derogatory information and/or targeting rules, or (b) when there are matches against derogatory information and/or targeting rules, but DHS does not object to the visa being issued. This retention period will allow HSI to revisit transaction activity for applicants that had previously been reviewed and only later found to be potential matches for criminal or terrorist activity.

(2) HSI will retain for 75 years after the date of review records of visa security reviews when (a) HSI and CBP do not object to the issuance of the visa but provide terrorism-related information to DOS regarding the applicant, or (b) HSI and CBP recommend against the issuance of a visa due to a nexus to terrorism. These records will be retained to support law enforcement and intelligence activities.

(3) Records for which HSI and CBP recommend against the issuance of a visa when there is no nexus to terrorism will be retained for 25 years after the date of review. Given the ten-year statute of limitations on visa-related crimes, it is important for HSI and CBP personnel to retain long-term case history for any investigations of visa fraud. In addition, the 25-year retention period for all of these records allows users to view previous casework on visas that were issued for ten-year multiple entry. This also enables users to view the visa encounter history when the person applies for a new visa.

[32] Pursuant to 5 U.S.C. §552a(e)(3), agencies are required to provide a Privacy Act Statement to individuals prior to the collection of PII that will be entered into a system of records. The purpose of a Privacy Act Statement is to identify how the Department will use the PII and provide transparency and notice to the person about whom PII is being collected.

Retaining these records for 25 years will also help facilitate legitimate travel and support investigative efforts.

5.2 Privacy Impact Analysis: Related to Retention

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 information in VSP-PATRIOT is retained for the time frames outlined in question 5.1. These retention periods help ensure visa application information is available to HSI and CBP for an appropriate period of time, thus facilitating their processing of future visa requests for the same applicant and any future investigative efforts related to the applicant. The retention periods are consistent with the retention periods for law enforcement systems and are appropriate given the HSI and CBP missions and the purpose of the VSP.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

As noted above, at select locations, HSI Special Agents manually upload a subset of the visa application data elements received from CEAC, which may include biographical, employment, and contact information about the visa applicant into a commercial third-party tool. The tool uses the subset of data to search against public-facing websites to determine a risk level of individuals for criminal or terrorism-related activities as well as provides a score indicating the confidence that the information is associated with the relevant visa applicant. Determination of risk from the internet searches does not, on its own, result in a negative recommendation. However, the results, documented in VSP-PATRIOT, supplement data in government holdings to determine those individuals that require further investigation.

HSI and CBP also share information from their visa security reviews with DOS in order to provide advice regarding specific security threats an individual may pose and a recommendation on whether or not to issue an individual's visa. This information is ingested into CCD, and DOS personnel access the information by logging onto CCD. DOS controls the categories of personnel who may access CCD.

If during the course of their review, HSI and CBP personnel discover a possible violation of a statute, rule, or regulation, HSI and CBP will also share VSP-PATRIOT information with the appropriate federal, state, local, or foreign agency responsible for investigating, prosecuting,

enforcing, or implementing the statute, rule, or regulation that appears to have been violated.[33] To the extent that the information is derived in whole or part from a DOS record, the disclosure will require authorization from a DOS representative.

If HSI and CBP personnel determine that a visa applicant has a nexus to terrorism during the screening and vetting process, the visa record is forwarded to the NCTC as mandated by the Intelligence Reform and Terrorist Prevention Act, Homeland Security Presidential Directive 6, and Executive Order 13388.

If HSI and CBP wish to share information from VSP-PATRIOT that consists of or is derived solely from a DOS visa record or a portion of such record, with entities outside of DHS, that information must be treated in accordance with the disclosure restrictions described in section 222(f) of the INA, and such sharing is further governed by the terms and conditions of the interagency agreements listed in Section 1.1 of this PIA.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The DHS/ICE-012 Visa Security Program Records SORN provides routine uses (e.g., G, I, J, L) that allow for the sharing of information that is within the scope of applicable law and compatible with the operation and mission of the VSP, the purpose of which is to identify individuals who may be ineligible for a U.S. visa because of criminal history, terrorism association, or other factors and convey that information to DOS, which decides whether to issue the visa.[34] For example Routine Use J allows the sharing of information with DOS in the processing of petitions or applications for benefits under the INA, and all other immigration and nationality laws including treaties and reciprocal agreements. In addition, the sharing of HSI and CBP data with DOS is supported by the interagency sharing agreements cited in Section 1.1.

6.3 Does the project place limitations on re-dissemination?

Information shared with DOS is maintained in CCD and DOS controls the categories of personnel who may access CCD. The interagency agreements between DOS and DHS do place

[33] *See* DHS/ICE-012 Visa Security Program (VSP), 74 FR 50228 (Sept. 30, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns. This includes law enforcement and investigative uses, specifically routine uses E, G, I, J, etc. VSP-PATRIOT interfaces with the other systems to document investigative information found during the application and interview screening and vetting phases.

[34] ICE recognizes that under Executive Order 13768, federal agencies no longer extend Privacy Act protections to non-U.S. persons. However, DHS Privacy Policy Guidance Memorandum 2017-01 instructs components to balance the public interest against the privacy rights of the individual before making disclosures of an individual's PII. Routine uses published in ICE's SORNs are a result of such balancing strategies and provide guidance to ICE operators regarding when PII can be shared with third parties. As ICE's disclosure needs evolve, ICE stakeholders reassess or perform additional balancing analyses to update routine uses, thus retaining their reliability as guidance for operators.

limits on re-dissemination by each agency. Each agency must get the approval of the other agency, in accordance with the third agency rule,[35] before sharing the other agency's information. For example, for information shared with other government agencies for enforcement purposes because of a possible violation of a statute, rule, or regulation, generally the recipient agency may not further disseminate the information from VSP-PATRIOT unless it first gets permission from HSI.[36] However, for terrorism information shared with NCTC, DHS does not place limits on re-dissemination as sharing of that information is permitted by various laws on counterterrorism and national security including the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,[37] Foreign Intelligence Surveillance Act (FISA) of 1978,[38] and Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans. Otherwise, if DOS wants to share DHS information, DOS needs to work with their DHS liaison to get DHS approval prior to sharing the DHS information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

VSP-PATRIOT retains a log of information that is sent via the automated interface. The log captures the transaction's unique identifier, the DHS recommendation, the entity to which the information was sent (DOS or CBP), an indicator whether the transmission was successful, and the date and time when the record was sent. The log also does not contain any personally identifiable information regarding the individual whose application was reviewed.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information may be delivered to agencies outside of DHS that do not have a need to know VSP-PATRIOT information.

Mitigation: In addition to sharing information in VSP-PATRIOT as part of the visa application review process with DOS, HSI and CBP personnel will share information in VSP-PATRIOT with NCTC and appropriate federal, state, local, or foreign agencies that need the information for law enforcement or intelligence purposes. As mentioned before, system users take annual security and privacy training that helps mitigate the risk that they will inappropriately share information. Additionally, the federal, state, local, or foreign agencies who receive VSP-PATRIOT information may not further disseminate the information unless they first get

[35] *See* 28 CFR 16.4.
[36] Memorandum of Understanding among U.S. Immigration and Customs Enforcement of the Department of Homeland Security and the Bureaus of Consular Affairs and Diplomatic Security of the Department of State on Roles, Responsibilities, and Collaboration at Visa Security Units Abroad (January 2011).
[37] Pub. L. 108-458.
[38] 50 U.S.C. § 1801 et seq.

permission from HSI. Access is limited to individuals who have a need to know the information and use it according to permitted purposes.

Section 7.0 Redress

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

Individuals seeking notification of and access to any record contained in VSP-PATRIOT, or seeking to contest its content, 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
Washington, D.C. 20536-5009
Phone: (866) 633-1182
Fax: (202) 732-4265
http://www.ice.gov/foia/

All or some of the requested information may be exempt from access pursuant to the Privacy Act or Judicial Redress Act (JRA) to prevent harm to law enforcement investigations or interests. Providing an individual access to records contained in the system could inform the individual 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 an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.[39]

Additionally, information in a VSP-PATRIOT record that consists of or is solely derived from a DOS visa record is subject to the confidentiality requirements of the INA section 222(f), which exempts particular information from being accessed and amended by the subject of the record.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

The right to request amendment of records under the Privacy Act of 1974 (5 U.S.C. §552a) (Privacy Act) is limited to United States citizens and lawful permanent residents. Executive Order

[39] *See* DHS/ICE-006-Intelligence Records System (IIRS), 75 FR 9233 (March 1, 2010), and Final Rule for Privacy Exemptions, 75 FR 12437 (March 16, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.

No. 13468, Enhancing Public Safety in the Interior of the United States, (January 25, 2017), which states: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information," precludes DHS from extending such rights by policy. The Judicial Redress Act of 2015 (Judicial Redress Act) (5 U.S.C. §552a note), which amended the Privacy Act, provides citizens of certain countries with access, amendment, and other redress rights under the Privacy Act in certain limited situations.[40]

All or some of the requested information may be exempt from correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests. Providing an individual access to records contained in VSP-PATRIOT could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal an investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.[41]

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedure for submitting a request to contest a record and/or correct information is outlined in the DHS/ICE-012 Visa Security Program Records SORN and in this PIA in questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals, including those listed as spouses or U.S. points of contact, will be unable to meaningfully participate in the use of their data as maintained in this system or determine whether the system maintains records about them.

Mitigation: This risk is unmitigated. Because this system has a law enforcement purpose, individuals' rights to be notified of the existence of data about them, to review the data to ensure it is correct, and to direct how that data may be used by HSI, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools will no

[40] The foreign countries and regional organizations covered by the Judicial Redress Act, as of February 1, 2017, include the European Union (EU) and most of its Member States. For the full list of foreign countries and regional organizations covered by the Judicial Redress Act, please visit the DOJ website https://www.justice.gov/opcl/judicial-redress-act-2015.

[41] *See* DHS/ICE-006-Intelligence Records System (IIRS), 75 FR 9233 (March 1, 2010), and Final Rule for Privacy Exemptions, 75 FR 12437 (March 16, 2010), *available at* https://www.dhs.gov/system-records-notices-sorns.

longer be useful. Permitting individuals to direct the agency's use of their information will similarly interfere with the intended law enforcement use of the system.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The auditing capability in VSP-PATRIOT captures user activity information associated with viewing, creating, updating, or deleting records, including information about the user that performed the activity. The system's auditing provides information adequately detailed to facilitate the reconstruction of events if a compromise or misuse of the system occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. The audit trails are reviewed by system administrators and the system's Information System Security Officer (ISSO) on a regular basis and when there is indication of system misuse. Any information indicating misuse of the system will be forwarded to the system owner and the Joint Intake Center (JIC) for review. Additionally, automated tools (i.e., Splunk) used by system administrators assist them in their monitoring, analysis, and reporting of suspicious activities in the system.

Managers in the VSP can query and monitor user activity by generating a User Activity Report to ensure that users are using the system appropriately. The User Activity Report provides information including a user's name, the number of times the individual attempted to log in for a requested timeframe, the number of applications vetted by the user during the requested time frame, the user's post assignments, and the user's assigned role(s). Having this information enables managers to oversee the work being done by users and to identify and address anomalies that occur.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All HSI and CBP personnel complete annual mandatory privacy and security training. Additionally, users receive specific training for the application that includes guidance on appropriate uses of the system as well as issues relating to data accuracy. ICE Privacy will coordinate with HSI to provide training on appropriate uses of social media and publicly available information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only authorized HSI and CBP personnel who require access as a part of the performance of their official duties will be granted access to VSP-PATRIOT. Access to VSP-PATRIOT is role-based and is appropriately limited according to the user's need-to-know and mission responsibility. To receive access to VSP-PATRIOT, an HSI or CBP supervisor must submit a signed request to an ICE account administrator asking that his or her user be granted access. As part of the request, the supervisor indicates the level of access the user needs based on the user's functional role and the user's post assignment, which determines the part of the world from which the user can see records. Users with a post assignment of "London," for example, would only see records assigned to the London post, whereas users reviewing all visa applications would be assigned to all posts. The request is sent to the ICE account administrator, who reviews the request and either grants or denies the individual access to the system. It should be noted that this process is used regardless of whether the individual is a government employee or contractor.

User roles determine what specific functions personnel are authorized to perform in VSP-PATRIOT. Below is a description of each user role:

1) Investigator – HSI Special Agents and CBP officers with this user role review visa applications at domestic and overseas DHS office locations. Investigator users have the ability to view an application; make notes regarding changes in hit type (i.e., false match, positive match, inconclusive match); submit expert advice regarding specific security threats relating to the adjudication of an individual visa application or class of applications; submit a recommendation to DOS to issue or deny a visa; create and save queries; and generate statistical reports.

2) Analyst – HSI and CBP analysts with this user role review visa applications at domestic and overseas DHS office locations. Analyst users can view and notate changes in hit type; document expert advice regarding specific security threats relating to the adjudication of an individual visa application or class of applications; create and save queries; and generate statistical reports.

3) Read-Only – Users with this user role are typically support personnel at domestic and overseas DHS office locations who support the work of the investigators and analysts. Read-only users are responsible only for researching trends in visa applications, generating reports, and/or providing system support. Read-only users can view information regarding an application; create and save queries; and generate statistical reports.

4) Account Administrator – There are five (5) account administrators and they are situated in the NCR. Users with this user role review user account requests; create, deactivate, and activate

user accounts; manage and maintain the system maintenance; and periodically review the user access list and disable user accounts for individuals who no longer requires access, in accordance with the System Security Plan. Administrators also can generate user and statistical reports and update reference data. Once a user is properly identified and authenticated by the system, the user is authorized to perform all functions commensurate with their official assigned role.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All information sharing agreements and MOUs pertaining to the VSP-PATRIOT system are first drafted and/or updated by the relevant program office. The ICE Privacy Division and the Office of Principal Legal Advisor are also engaged to ensure that any privacy and legal risks are appropriately addressed. Prior to the agreement being sent to DHS for formal review, the document is reviewed by the other agency joining with ICE in the agreement.

Responsible Officials

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

Approval Signature Page

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

_____

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