Privacy Impact Assessment
for the

Visa Security Program Tracking System-Network version 2.0

DHS/ICE/PIA-011(a)

January 17, 2013

Contact Point
James Dinkins
Executive Associate Director
Homeland Security Investigations
Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(703) 343-1717

Abstract

The Visa Security Program Tracking System-Network (VSPTS-Net) is a U.S. Immigration and Customs Enforcement (ICE) case management system designed to support the activities of the ICE Visa Security Program. ICE originally deployed VSPTS-Net in 2010, and is now upgrading the system with the release of VSPTS-Net 2.0, which further modernizes and automates the visa security screening process. With VSPTS-Net 2.0, the Visa Security Program allows ICE and U.S. Customs and Border Protection (CBP) personnel to identify applicants for U.S. visas who are ineligible to enter the United States due to criminal history, terrorism associations, or other security-related grounds. ICE and CBP use VSPTS-Net 2.0 to record, track, and manage all in-depth visa security reviews performed by the agencies. ICE is conducting this Privacy Impact Assessment (PIA) because the release of VSPTS-Net 2.0 changes the way that personally identifiable information (PII) about individuals is collected, processed, and shared with other agencies.

Overview

VSPTS-Net[1] is owned by the ICE Office of Homeland Security Investigations (HSI), which also operates the Visa Security Program. VSPTS-Net is being replaced by VSPTS-Net 2.0, which supports the visa security work performed by HSI special agents and analysts (hereafter referred to as "HSI agents/analysts") and CBP officers and analysts (hereafter referred to as "CBP officers/analysts")[2] located domestically and at U.S. embassies, consulates, and offices abroad. The system is a globally accessible web-based application that manages the workflow associated with the Visa Security Program, and enables users to review visa applications with the objective of identifying applicants who are ineligible to enter the United States on security-related grounds. After reviewing an application, an HSI agent or CBP officer notifies the U.S. Department of State (DOS) with a recommendation regarding the issuance of the visa. VSPTS-Net 2.0 will replace VSPTS-Net and the data in VSPTS-Net will be migrated to VSPTS-Net 2.0.

Original Visa Security Program and VSPTS-Net System

In support of Section 428 of the Homeland Security Act of 2002, 6 U.S.C. § 236, ICE established the Visa Security Program and, as part of the program, HSI agents/analysts at U.S. embassies and consulates ("consular posts") in high-risk areas worldwide conduct security reviews of visa applications. They examine visa applications, investigate applicants who may be ineligible for a visa, coordinate with other law enforcement entities, and provide information and a recommendation back to DOS regarding individuals on whose visa applications DOS has already provided an initial issuance decision, but have not yet received their visa from DOS. The original VSPTS-Net application is used by HSI agents/analysts at consular posts to record, track, and manage the visa security reviews they perform on visa applications and to communicate the results to DOS officials.

[1] *See* DHS/ICE/PIA-011, Visa Security Program Tracking System PIA, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_vsptsnet.pdf.
[2] Analysts may be either federal employees or contractors.

In response to a congressional mandate, in May 2007, ICE created a Security Advisory Opinion Unit ("SAO Unit") within the Visa Security Program at ICE Headquarters to handle Security Advisory Opinions (SAO) requests issued by DOS. When DOS has security-related concerns regarding a visa application that ICE has already reviewed, DOS issues an SAO request on the application. The request is sent to various federal agencies, including ICE, which perform in-depth reviews of the security-related concerns identified by DOS. ICE's SAO Unit responds to SAO requests and provides DOS with information held by the U.S. Department of Homeland Security (DHS) on the visa applicant that may be relevant to the applicant's eligibility for a visa, such as information regarding the applicant's criminal or terrorism background or other derogatory information that may be relevant. VSPTS-Net is used by the SAO Unit to record, track, and manage the visa security reviews they perform and to communicate the results to DOS.

The original VSPTS-Net application helps DHS and DOS prevent known and suspected terrorists, criminals, and other ineligible persons from obtaining U.S. visas. It provides HSI agents/analysts with a system for managing the workflow associated with visa security reviews and provides the necessary analytical, reporting, and data storage capabilities the program requires. VSPTS-Net receives visa applications and SAO requests from the DOS Consular Consolidated Database (CCD), which is the official repository of visa records from U.S. consular posts around the world.[3] VSPTS-Net receives a data extract of visa applications from CCD that an HSI agent/analyst loads into TECS, a DHS system that contains law enforcement information including law enforcement, immigration, border, and lookout records.[4] The applications are screened in TECS to determine if the applicant has a criminal or terrorism background, a record of immigration violations, or other derogatory information that may be relevant to the applicant's eligibility for a visa under federal law. The VSPTS-Net user then manually logs the TECS screening results into VSPTS-Net, adds relevant notes including derogatory information about the applicant, and makes a recommendation for DOS regarding the issuance of the visa to the individual (e.g., no objection to DOS's initial issuance decision; recommend that the visa not be issued). (Note: only HSI agents can make recommendations to DOS.) VSPTS-Net generates a Daily Report that is emailed to DOS that lists the various visa applications and SAO requests that were processed that day. The report provides information about the application including the applicant's name and date of birth; the ICE recommendation; the relevant code of law if ICE is recommending that the visa application be denied; and any summary notes.

VSPTS-Net 2.0

With the release of VSPTS-Net 2.0, the Visa Security Program is changing in several ways. First, CBP officers/analysts will join HSI agents/analysts to screen visa applications and determine whether or not visas should be issued. More of this work will also be performed from locations in the United States rather than at consular posts. Second, all visa applications worldwide, not just those from high risk areas

[3] For additional information, see the State Department's CCD PIA (Dec. 11, 2008), at http://www.state.gov/documents/organization/93772.pdf.
[4] *See* DHS/ CBP/PIA-009, TECS System: CBP Primary and Secondary Processing PIA, at http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs.pdf

of the world, will be screened using VSPTS-Net 2.0. Third, the visa screening process will be changed to allow ICE's visa recommendation to occur and be communicated to DOS personnel prior to DOS's initial decision on the visa. Under the current process, the ICE visa recommendation occurred and was communicated to DOS after the initial visa decision was made but before the visa was physically issued.

Under the new process supported by VSPTS-Net 2.0, the visa applicant first completes his or her visa application in paper or via the DOS Consular Electronic Application Center (CEAC) system.[5] The visa application information is then passed to CCD, which sends it to the CBP Automated Targeting System (ATS)[6] before DOS personnel review the application. ATS screens the visa application information against derogatory information[7] and targeting rules[8] in ATS, and determines if there are any possible matches. ATS then sends the visa application information and the ATS screening results to VSPTS-Net 2.0 via the automated system-to-system interface between ATS and VSPTS-Net 2.0. If there are matches to the derogatory information for the visa applicant, the screening results sent to VSPTS-Net 2.0 provide the name of the system that was the source of the derogatory information about the applicant and the data element(s) for which there was a match, e.g., the applicant's date of birth, home address, or passport number. The actual value of the data element for which there was a match is not sent. If there are matches to targeting rules, the screening results provide an identifier for the targeting rule and a brief explanation of the rule, such as "terrorism activity." The targeting rules are not sent to VSPTS-Net 2.0. As a part of the standard visa issuance process, visa applicants are required to appear at the visa issuing consulate for an interview with a DOS official. When the visa applicant comes to the consulate for this interview, a DOS official will verify and update, 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. ATS then sends the updated visa application information and ATS screening results to VSPTS-Net 2.0.

If there is no match to derogatory information and/or targeting rules, VSPTS-Net 2.0 will send an automatic response to CCD using the automated system-to-system interface between the two systems with a "No Objection" recommendation from DHS regarding the issuance of a visa to the applicant.

For initial applications or applications updated after the interview that are identified during the ATS screening as possible matches against derogatory information and/or targeting rules, VSPTS-Net 2.0 will flag those applications for review by HSI agents/analysts and CBP officers/analysts, who will determine if 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. While ICE and CBP personnel are

[5] For more information on the CEAC system, see http://www.state.gov/documents/organization/99026.pdf.
[6] *See* DHS/CBP/PIA-006 Automated Targeting System PIA and PIA updates at http://www.dhs.gov/privacy-documents-us-customs-and-border-protection. See DHS/CBP-006 Automated Targeting System SORN, May 22, 2012, 77 Fed. Reg. 30297 at http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.
[7] Derogatory information is information about individuals such as their date of birth, home address, passport number, or e-mail address that is sent to ATS by other systems such as TECS. The derogatory information is used by ATS for screening purposes.
[8] Targeting rules are criteria developed by DHS from trend analysis, law enforcement cases, and intelligence used for screening purposes.

reviewing the visa application, they may contact HSI agents at consular posts to assist them by performing investigations in their local area regarding the applicant, by working with local law enforcement officials, or by interviewing the applicant at the consular post. ICE and CBP personnel will record information related to their reviews and recommendations in VSPTS-Net 2.0. VSPTS-Net 2.0 will then send the DHS visa recommendation to CCD and ATS via automated system-to-system interfaces. The system will also send with the visa recommendation a summary of relevant notes; the application's request identifier and its DOS-issued bar code; and the relevant code(s) of law (if DHS is recommending that the visa application be denied). Note: only HSI agents and CBP officers will make recommendations to DOS. Using the information provided to CCD, DOS then makes its initial visa issuance decision. If DOS has security-related concerns regarding the visa application and issues an SAO request, the application will again be sent to ATS and using the process described above, ICE and CBP will review it and provide a recommendation to DOS.

Although VSPTS-Net 2.0 will automatically send visa recommendations to CCD, VSPTS-Net 2.0 will still generate the Daily Report, to be used as a back-up option if the automatic interface with CCD is inoperable as well as for internal DHS reporting purposes. After DOS makes it final decision and either issues or denies the visa, CCD updates TECS with DOS' final determination. ATS receives the final determination from TECS and passes this information to VSPTS-Net 2.0, which then completes and closes the record of the visa security review.

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?

ICE operates VSPTS-Net 2.0 pursuant to Section 428 of the Homeland Security Act of 2002, 6 U.S.C. § 236, 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." VSPTS-Net 2.0 allows ICE and CBP personnel to identify those applicants for U.S. visas who are ineligible to enter 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 refusal determinations.

In addition, it 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 and passport records and immigration and 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 State Department with DHS is subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA) (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, 74 Fed. Reg. 50228 (Sept. 30, 2009), applies to the information in VSPTS-Net.[9]

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

The original VSPTS-Net system had a Security Plan (SP) that was completed and approved as a result of the Security Authorization (replaces Certification and Accreditation [C&A]) on February 5, 2010. An updated version of the SP in support of VSPTS-Net 2.0 will be approved during the next re-authorization process scheduled for completion at the end of 2012.

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

Yes. The records retention schedule was approved by NARA in February 2010, but the schedule is being updated.

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 agents/analysts and CBP officers/analysts do not perform "collections of information" from the public in support of the Visa Security Program, therefore this activity is not covered by PRA.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

[9] *See* DHS/ICE-012 Visa Security Program (VSP) SORN at http://www.gpo.gov/fdsys/pkg/FR-2009-09-30/html/E9-23522.htm.

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

DOS collects information directly from visa applicants as part of the visa application process that is then provided to DHS (ATS and VSPTS-Net 2.0). Data collected from visa applications includes, but is not limited to:

- Biographic information about the applicant including name, address, phone number, email address, date of birth, country of birth, nationality;
- Information about other individuals 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, 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; and
- Security and background-related information[10] 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 intention to engage in espionage or terrorist activities); and
    - Immigration-related information (for example, previous deportations, removals, or overstays).

VSPTS-Net 2.0 uses and maintains any information provided by an individual applying for a U.S. visa except Social Security Number (SSN), Alien Registration Number (A-Number), U.S. Driver's License Number, and U.S. Taxpayer ID. During the ingestion of visa application information into VSPTS-Net 2.0 from ATS, VSPTS-Net 2.0 performs a system check to ensure that these data elements are not ingested into the system.

Additionally, if there are no matches against derogatory information or targeting rules for the visa applicant, ATS sends VSPTS-Net 2.0 an indication that there were no matches. If there are matches to the derogatory information, the screening results sent to VSPTS-Net 2.0 provide the name of the system that was the source of the derogatory information about the applicant, any relevant system identifiers from the source system, and the data element(s) upon which there was a match, e.g., the applicant's date of birth,

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

home address, or passport number. Note: the actual value of the data element for which there was a match is not sent. If there are matches to targeting rules, the screening results provide an identifier for the targeting rule and a brief explanation of the rule, such as "terrorism activity."

In addition to information about the visa applicant, VSPTS-Net 2.0 will also maintain any relevant information the applicant provides during the DOS visa interview, as well as additional information gathered such as a description of any irregularities with the physical passport. An example of information that an applicant may provide during an interview that is recorded into VSPTS-Net 2.0 could be information on places the applicant intends to visit in the United States.

The system will maintain information compiled by HSI agents/analysts and CBP officers/analysts when reviewing the application including an applicant's criminal history, visa, and immigration history information; information relating to the individual's involvement in terrorism or other national security issues; and the DOS-issued bar code and request identifier for the visa application. VSPTS-Net 2.0 also maintains the final 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. Additionally, the system has limited identifying and contact information about the agents, officers, and analysts that conducted the visa security review.

As noted above, if the automated interface with CCD is down, the Daily Report will be e-mailed to DOS after it has been encrypted and password protected. The Daily Report contains information to identify the applicant (name and date of birth), numeric identifiers from the government IT systems, DHS's visa recommendation and any supporting legal citations, and DHS's summary notes about findings regarding the applicant.

VSPTS-Net 2.0 also enables users to generate other reports in support of the Visa Security Program. 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 where there was a conflict between the DHS recommendation and DOS decision.

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 and ingested into the DOS CCD system. CCD sends the data to ATS for screening and additional information about possible matches to derogatory information and/or targeting rules may be added. HSI agents/analysts and CBP officers/analysts may also obtain information through queries of other Federal databases including but not limited to ICE Pattern Analysis and Information Collection System (ICEPIC), DHS/ICE-002 (73 Fed. Reg. 48226, August 18, 2008),[11] US-VISIT's Arrival Departure Information System (ADIS), DHS/USVISIT-001 (72 Fed. Reg. 47057, August 22, 2007),[12] ICE's Student and Exchange Visitor

[11] For more information about DHS/ICE-002 ICEPIC SORN, see http://www.gpo.gov/fdsys/pkg/FR-2008-08-18/html/E8-19031.htm.
[12] For more information about DHS/USVISIT-001 ADIS SORN, see http://www.gpo.gov/fdsys/pkg/FR-2007-08-

Information System (SEVIS), DHS/ICE-001 (75 Fed. Reg. 412, January 5, 2010),[13] and ICE's Immigration and Enforcement Operational Records System (ENFORCE), DHS/ICE-011 (75 Fed. Reg. 23274, May 3, 2010).[14] 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.

All transmission of data between ATS, CCD, and VSPTS-Net 2.0 occurs via secure electronic system-to-system connections.

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

HSI agents/analysts and CBP officers/analysts may use information from open source sites including from social media sites and commercial data aggregators in the course of their reviews, but those systems will not interface with VSPTS-Net 2.0. ICE and CBP personnel 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. ICE and CBP personnel may choose to include the information found on public websites in the visa applicant's file.

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 on the visa application and during the visa interview process. Because this information is collected from the individual, it is generally deemed to be highly accurate and reliable. Second, the automated system-to-system interfaces among CCD, ATS, and VSPTS-Net 2.0 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 performed by ICE and CBP personnel against federal databases and publicly available websites help to identify potential inconsistencies or inaccuracies in the data. All of these factors contribute to greater data accuracy.

22/html/E7-16473.htm.

[13] For more information about DHS/ICE-001 SEVIS SORN, see http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/html/E9-31268.htm.

[14] For more information about DHS/ICE-011 ENFORCE SORN, see http://www.gpo.gov/fdsys/pkg/FR-2010-05-03/html/2010-10286.htm.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that ICE will receive more information about visa applicants than is necessary to accomplish the purposes of the Visa Security Program.

Mitigation: Only information relevant to the visa application review is added to VSPTS-Net 2.0. Any SSNs, A-Numbers, Driver's License Numbers, or U.S. Taxpayer IDs that may accompany applications are not ingested into VSPTS-Net 2.0 from ATS. Access to VSPTS-Net 2.0 is strictly enforced and accounts are granted on a strict need-to-know basis.

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 biometric and biographic checks are performed against government data systems. Second, ICE, CBP, and DOS personnel review the information collected about visa applicants and others during the visa security review before a final decision is made on an application. Finally, ICE and CBP personnel check 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 not attributed to the wrong individual, and if incorrect information is identified, ICE and CBP personnel can correct it before DOS makes a final determination on the visa application.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of 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 decision is made, and make a recommendation to DOS on the visa decision. ICE 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 VSPTS-Net 2.0 including any information ICE 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. First, they use it 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 ICE and CBP personnel assigned to the Visa Security Program. Second, they use it to enhance the screening criteria used by ATS. CBP uses the information provided to identify trends that can establish and/or modify targeting rules. Additionally, the information sent by VSPTS-Net 2.0 is added to the derogatory information against which ATS screens visa applications. The enhancements to ATS screening are designed to help identify the visa applicant if he or she reapplies or to identify people associated with the applicant.

The information is also used to manage and prioritize the work of ICE and CBP personnel assigned to the Visa Security Program. Once visa applications have been screened against ATS, applications that possibly match derogatory information and/or targeting rules are flagged in order to be more thoroughly reviewed by ICE and CBP personnel. Applications that have been flagged are prioritized in VSPTS-Net 2.0 by the type of match so that high priority applications such as terrorist-related matches are reviewed first. The information in the system and the metrics developed about the Visa Security Program are shared with other DHS offices at locations abroad and with ICE headquarters to facilitate visa security reviews and oversight of the program.

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. VSPTS-Net 2.0 is a case management tool used to document information found during reviews and send and receive information to other U.S. Government systems during the visa security process.

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

Yes. VSPTS-Net 2.0 is used by both HSI agents/analysts and CBP officers/analysts as the case management tool for the DHS visa vetting security process. ICE and CBP personnel assigned to support the Visa Security Program have the permissions needed to review visa applications and to provide feedback and recommendations (refusal, revocation, no objection) to DOS and CBP.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized disclosure of information in the system by users.

Mitigation: In the standard operating procedures for VSPTS-Net 2.0 and in the 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 ICE and CBP personnel must take annual computer security and privacy training. Individuals who are found to have accessed or used the VSPTS-Net 2.0 data in an unauthorized manner will be disciplined appropriately. In addition, ICE conducts regular audits of VSPTS-Net 2.0 users and their use of the system and maintains an audit trail of activity in the system.

Privacy Risk: There is a risk of misuse by authorized users.

Mitigation: The risk that VSPTS-Net 2.0 information will be misused 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 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, ICE conducts regular self-audits of users and maintains an audit trail of activity in the system.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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. Additionally, the DHS/ICE-012 Visa Security Program Records SORN and this PIA along with the DOS/STATE-39 Visa Records SORN[15] 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. 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 denial of visa services because the U.S. does not have all the information it needs in order 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.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that applicants 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 thus making the individual aware of the information that is being collected. Applicants also receive notice through this PIA and the Visa Security Program Records SORN. These provide the individual with notice on the information that is collected and on how the information is used and shared.

[15] For more information, see http://www.state.gov/documents/organization/102815.pdf.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Several different categories of records are retained in VSPTS-Net 2.0 with varying retention periods.

(1) Records of visa security reviews will be retained for 25 years after the date of review for records which (a) ICE and CBP do 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 ICE and CBP 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) ICE will retain for 75 years after the date of review records of visa security reviews when (a) ICE and CBP do not object to the issuance of the visa but provide terrorism-related information to DOS regarding the applicant, or (b) ICE and CBP recommend against the issuance of a visa due to a nexus to terrorism. These records will be retained in order to support law enforcement and intelligence activities.

(3) Records for which ICE 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 ICE and CBP personnel to have 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. 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 VSPTS-Net 2.0 is retained for the time frames outlined in question 5.1. These retention periods help ensure visa application information is available to ICE 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 ICE and CBP missions and the purpose of the Visa Security Program.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other Federal, state, and local governments and private sector entities.

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, ICE and CBP 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 the DOS CCD system, 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, ICE and CBP personnel discover a possible violation of a statute, rule, or regulation, ICE and CBP will also share VSPTS-Net 2.0 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. 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. As part of the disclosure process, ICE and CBP personnel will also make an accounting for the disclosure.

If ICE 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 National Counterterrorism Center (NCTC) as mandated by the Intelligence Reform and Terrorist Prevention Act, Homeland Security Presidential Directive 6, and Executive Order 13388. An accounting for the disclosure is made. (Note: accountings for disclosure will not be kept in VSPTS-Net 2.0.)

If ICE and CBP wish to share information from VSPTS-Net 2.0 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 Privacy Impact Assessment.

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 that allow for the sharing of information that is associated with the operation and mission of the Visa Security Program. In addition, the sharing of ICE 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?

As noted above, 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 limits on re-dissemination by each agency. With two limited exceptions, each agency must get the approval of the other agency before sharing the other agency's information. So, for example, 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.

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 VSPTS-Net 2.0 unless it first gets permission from ICE.

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, P.L. 108-458, Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1801 *et seq*, and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*.

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

VSPTS-Net 2.0 retains a log of information that is sent via the automated interface to DOS and CBP. 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 does not contain any personally identifiable information regarding the individual whose application was reviewed.

For Daily Reports that are generated in VSPTS-Net 2.0 and emailed to DOS, an ICE group mailbox is carbon copied on the email to DOS in order to record what was sent. For information that is sent to outside agencies, ICE and CBP personnel make an accounting for the disclosure.

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 VSPTS-Net 2.0 information.

Mitigation: In addition to sharing information in VSPTS-Net 2.0 as part of the visa application review process with DOS, ICE, and CBP personnel will share information in VSPTS-Net 2.0 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 VSPTS-Net 2.0 information may not further disseminate the information unless they first get permission from ICE.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress, which may include access to records about themselves, ensuring the accuracy of the information collected about them and/or filing complaints.

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

Individuals seeking notification of and access to any record contained in VSPTS-Net 2.0, or seeking to contest its content, may submit a request in writing to the ICE 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 in order 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. *See* 75 Fed. Reg. 12437 (Mar. 16, 2010).

Additionally, information in a VSPTS-Net 2.0 record that consists of or is solely derived from a DOS visa record is subject to the confidentiality requirements of 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 correction procedures are identical to those described in Question 7.1 above. All or some of the requested information may be exempt from correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing an individual access to records contained in VSPTS-Net 2.0 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. *See* 75 Fed. Reg. 12437 (Mar. 16, 2010).

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

The procedure for submitting a request to 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 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: 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 ICE, 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 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

The following questions are intended to describe technical and policy based safeguards and security measures.

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

The auditing capability in VSPTS-Net 2.0 captures user activity information associated with viewing, creating, updating, or deleting records including 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. Additionally, automated tools used by system administrators assist them in their monitoring, analysis, and reporting of suspicious activities in the system.

Managers in the Visa Security Program are able to query and monitor user activity by generating the 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 login for a requested timeframe, the number of applications vetted by the user during the requested time frame, the user's post(s) 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 ICE and CBP personnel complete annual mandatory privacy and security training. Additionally, users receive specific training for the application which includes guidance on appropriate uses of the system as well as issues relating to data accuracy.

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 VSPTS-Net 2.0. Access to VSPTS-Net 2.0 is role-based and is appropriately limited according to the user's need-to-know and mission responsibility. To receive access to VSPTS-Net 2.0, an ICE or CBP supervisor must submit a signed request 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 individual'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 an 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 users are authorized to perform in VSPTS-Net 2.0. Below is a description of each user role:

1) Investigator - HSI 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, update, and make changes to information regarding an application; 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 – CBP and HSI analysts with this user role review visa applications at domestic and overseas DHS office locations. Analyst users have the ability to view, update, and make changes to information regarding an application; 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 have the ability to view information regarding an application; create and save queries; and generate statistical reports.

4) Account Administrator – 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. Administrators also have the ability to generate user and statistical reports and update reference data. Users with this user role are assigned to all posts.

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 VSPTS-Net 2.0 system are first drafted and/or updated by the relevant program office. The ICE Privacy Office 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

Lyn Rahilly, Privacy Officer
U.S. Immigration & 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