Privacy Impact Assessment
for the

Visa Security Program Tracking System

August 27, 2009

Contact Point
Raymond R. Parmer
Director, Office of International Affairs
U.S. Immigration and Customs Enforcement
(202) 732-0350

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Visa Security Program Tracking System (VSPTS-Net) is a U.S. Immigration and Customs Enforcement (ICE) system that supports the management of ICE's Visa Security Program, which seeks 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 Special Agents use VSPTS-Net to record, track, and manage all visa security reviews performed by ICE. ICE conducted this PIA because VSPTS-Net collects personally identifiable information (PII) about individuals that have applied for U.S. visas.

Overview

VSPTS-Net is owned by the ICE Office of International Affairs (OIA). VSPTS-Net provides ICE Agents located at U.S. embassies and consulates abroad with a globally accessible web-based application to manage the workflow associated with OIA's Visa Security Program (VSP), which investigates visa applications. VSPTS-Net is scheduled to launch in September 2009. With the deployment of VSPTS-Net, ICE will retire the predecessor system known as the VSP Tracking System. Concurrently with the publication of this PIA, ICE is also publishing a Privacy Act System of Records Notice (SORN) describing the information ICE maintains in VSPTS-Net and through the Visa Security Program.

Visa Security Program

In support of Section 428 of the Homeland Security Act of 2002, ICE deploys agents to U.S. embassies and consulates ("consular posts") in high-risk areas worldwide to conduct security reviews of visa applications. ICE agents assigned to VSP ("VSP agents") examine visa applications in-depth, investigate applicants who may be ineligible for a visa, coordinate with other law enforcement entities, and provide advice and training to the State Department. The purpose of VSP is to provide expert advice to State Department officials regarding specific security threats relating to the adjudication of individual visa applications or classes of applications. VSPTS-Net is used to support ICE's VSP activities, in particular to record, track, and manage the visa security reviews conducted at consular posts and to communicate the results to State Department officials.

In response to a congressional mandate, in May 2007, ICE created a Security Advisory Opinion Unit ("SAO Unit") within VSP at ICE Headquarters. A Security Advisory Opinion (commonly referred to as an "SAO") is a U.S. Government mechanism to coordinate third-agency checks on visa applicants about whom the State Department have security-related concerns. Applicants identified for an SAO require in-depth review by multiple federal agencies. The State Department provides the results of SAO checks to consular officers to aid in adjudicating visa applications. ICE's SAO Unit responds to SAO requests generated worldwide and conducts a visa security review which provides the State Department with DHS-held information on visa applicants. The purpose of the SAO Unit is to integrate VSP's law enforcement expertise into the current SAO process. VSP agents and analysts in the SAO Unit conduct visa security reviews on applicants who may be ineligible for a U.S. visa because of criminal history, terrorism association, or other factors and convey that information to the State Department which decides whether to issue the visa. VSPTS-Net is also used to support VSP's SAO Unit activities, in particular to

record, track, and manage the visa security reviews initiated through the SAO process and to communicate the results to the State Department.

VSPTS-Net

VSPTS-Net provides VSP agents with an intranet-based system that manages the workflow associated with visa security reviews and provides the necessary analytical, reporting and data storage capabilities VSP requires. VSPTS-Net allows users (ICE employees and contractors) to record relevant visa application data, derogatory information about applicants, and visa recommendation data. It also supports the generation of performance metrics for the VSP program as a whole. Ultimately, the system helps VSP and the State Department prevent known and suspected terrorists, criminals, and other ineligible persons from obtaining U.S. visas. The initial release of the system does not directly exchange information with other systems.

Prior to the deployment of VSPTS-Net, VSP agents used the VSP Tracking System to manage the visa screening and vetting work they performed. The VSP Tracking System consisted of several standalone databases located at each consular post. While this system helped agents manage their VSP workload and record their work, its architecture prevented the sharing of information within ICE, resulting in inefficiencies. VSPTS-Net provides greater support to VSP by allowing agents to share visa security review information directly with other VSP agents consular posts and with ICE Headquarters. VSPTS-Net will also allow ICE to track and manage VSP performance and metrics in an effective manner across the various geographic locations.

VSPTS-Net receives information from the State Department's Consular Consolidated Database (CCD), which is the official repository of visa records from U.S. consular posts around the world.[1] CCD supplies VSPTS-Net with visa applicant data for particular high-risk consular posts, which allows ICE to identify visa applicants who require further investigation. ICE then uses TECS, a Department of Homeland Security (DHS) system[2] that contains law enforcement, immigration, border, and lookout records, 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.[3] VSPTS-Net reformats the data received from CCD and provides an extract to the agent. The agent loads the extract into TECS where it queries the visa applicants' identifying data against TECS. TECS also connects to and queries against the Federal Bureau of Investigation's National Crime Information Center (NCIC), which contains various law enforcement records (such as records of criminal wants and warrants) supplied by Federal, state, local, and foreign law enforcement agencies.

Typical Transaction

VSP agents at consular posts begin each day by conducting an initial review of new applicants for U.S. visas. First, agents electronically compare visa applicant information obtained from State Department's CCD against lookout, law enforcement and immigration records in TECS to determine

[1] For additional information, see the State Department's CCD PIA (Dec. 11, 2008), www.state.gov/documents/organization/93772.pdf.
[2] *See* U.S. Customs and Border Protection (CBP) TECS Privacy Act System of Records Notice, DHS/CBP-011, 73 FR 77778, Dec. 19, 2008.
[3] Lookout records are records in TECS that flag individuals for additional action when encountered by DHS officers.

which applicants require further investigation. Extracts from CCD containing the applicant information (applicant name, passport number and date of birth) are manually loaded into VSPTS-Net, which reformats the data before it is manually loaded into TECS. VSP agents review in TECS any matching TECS or NCIC records against the applicant data. Using VSPTS-Net, VSP agents also sort visa applicant information to identify those that meet security criteria that varies by consular post which indicates they are at a high risk of visa ineligibility. Based on these analyses, VSP agents identify which applicants do or do not require further investigation and make notations in VSPTS-Net accordingly. For applicants who are selected for further investigation, VSP agents may conduct applicant interviews, additional database checks, a physical document review, and liaison with local law enforcement officials, among other types of investigative activities. VSP agents make notations in VSPTS-Net of these activities and the information gathered. Once the visa security review is complete, VSP agents enter ICE's advice into VSPTS-Net. VSPTS-Net generates daily reports that ICE emails to the State Department that contain ICE's expert advice regarding specific security threats relating to the adjudication of individual visa applications or classes of applications and recommendations for the issuance of U.S. visas. State Department officials then make the visa decisions and notify the applicants of the results. The VSP recommendation and the State Department decision are both recorded in VSPTS-Net.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

VSPTS-Net collects, uses, disseminates, and maintains all information provided by an individual applying for a U.S. visa. The State Department provides multiple visa application forms, but the primary visa application forms used are the State Department Form DS-156 for non-immigrant visa applicants and the State Department Form DS-230 for immigrant visa applicants. VSP also retains data from other forms used in the visa application process. Data collected from the application includes, but is not limited to, the applicant's name, address, phone number, email, date of birth, country of birth, nationality, and passport number.

In addition, information on other individuals is collected from the visa application including the applicant's spouse, individuals traveling with applicant, application preparer's name, and the applicant's point of contact in the United States, if any. VSPTS-Net will also maintain any relevant information the applicant provides during the visa interview, as well as descriptions of any irregularities with the physical passport. An example of information that an applicant may provide that is recorded into VSPTS-Net could be information on places the applicant intends to visit in the United States.

The applicant's criminal history, visa and immigration history, State Department-issued visa control number, and information relating to terrorism and national security will also be noted within

VSPTS-Net. VSPTS-Net will maintain the expert advice of the VSP agent and the State Department's final visa decision. The system will maintain limited identifying and contact information about the VSP agent that conducted the visa security review.

1.2 What are the sources of the information in the system?

Visa applicant data is obtained primarily from CCD and applicant interviews, and related lookout data from TECS, DHS/CBP-011, (73 FR 77778, Dec. 19, 2008), and NCIC. VSP agents may also obtain information through queries of other Federal databases during the course of a visa security review, including ICE Pattern Analysis and Information Collection System (ICEPIC) DHS/ICE-002 (73 FR 48226, Aug. 18, 2008), CBP's Automated Targeting System (ATS) DHS/CBP-006, (72 FR 43650, Aug. 6, 2007), US-VISIT's Arrival Departure Information System (ADIS) DHS/USVISIT-001, (72 FR 47057, Aug. 22, 2007), ICE's Student and Exchange Visitor Information System (SEVIS) DHS/ICE-001, (70 FR 14477, Mar. 22, 2005), and ICE's Enforcement Operational Immigration Records (ENFORCE) DHS/ICE-CBP-CIS-001-03, (71 FR 13987, Mar. 20, 2006). Agents may also obtain information from other sources during the review, including foreign governments, Interpol, Europol, employers, public records, family members, and other individuals and entities that may be interviewed or serve as the source of information.

1.3 Why is the information being collected, used, disseminated, or maintained?

This information is necessary for ICE to conduct visa security reviews, and to provide State Department officials with expert advice regarding specific security threats relating to the adjudication of individual visa applications or classes of applications and a visa recommendation or information relevant to the applicant's eligibility for a visa under Federal law.

1.4 How is the information collected?

The State Department collects information from the visa applicant using its own visa application forms and during the visa interview. State Department personnel enter this information into State Department consular systems that feed into CCD. The VSP agent logs in to CCD, extracts the visa application information for his or her consular post as an Excel file, and saves it to his or her ICE computer. The agent then imports the Excel file into VSPTS-Net, which reformats it into a .txt file that allows the information to be screened as a batch file in TECS. The .txt file is saved to the VSP agent's ICE computer and uploaded into TECS. Finally, the VSP agent runs a batch matching program comparing the visa applicant data in the .txt file against the records in TECS, and views the results in TECS. Any pertinent derogatory information from TECS, other databases, law enforcement agencies, applicant interviews, and other sources will be manually typed into VSPTS-Net by the VSP agent.

1.5 How will the information be checked for accuracy?

The government agency that originally collected the data is responsible for ensuring data accuracy. The State Department collects information from the visa applicant using visa application forms and during the visa interview process. Because this information is collected from the individual, it is generally deemed to be highly accurate. Accuracy of this data will be further confirmed through biometric-based checks run by the State Department through the US-VISIT program, which compares biometrics of visa applicants against existing U.S. biometric databases. VSP agents' checks against TECS and other databases will also help to identify potential inconsistencies or inaccuracies in the data, which can then be resolved by the VSP agent.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

ICE operates the VSP pursuant to Section 428 of the Homeland Security Act of 2002 and 22 C.F.R. 41.122. In addition, VSP is supported by the Memorandum of Understanding (MOU) between DHS, Federal Bureau of Investigation, and State Department Bureau of Consular Affairs on Improved Information Sharing Services, signed July 18, 2009, and the MOU between the Secretaries of State and Homeland Security concerning the implementation of Section 428 of the Homeland Security Act of 2002, signed by the Secretary of State and the Secretary of Homeland Security on September 26, 2003, which governs the implementation of Section 428 by these agencies.

The disclosure and sharing of visa record information by the State Department with the Department of Homeland Security is subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA) (8 U.S.C. 1202(f)).

This data sharing arrangement is further governed by the terms and conditions of the Memorandum of Agreement (MOA) between the State Department and the Department of Homeland Security regarding the sharing of visa and passport records and immigration and naturalization and citizenship records (hereafter, DOS-DHS MOA), signed by the Assistant Secretary of Consular Affairs and the Assistant Secretary of the Office of Policy on November 18, 2008, as well as the MOU between the State Department, Bureau of Consular Affairs and the Department of Homeland Security, U.S. Immigration and Customs Enforcement for Cooperation in Datasharing (Visa and Immigration Data) (hereafter, CA-ICE MOU), signed by the Assistant Secretary of Consular Affairs and the Assistant Secretary of Immigration and Customs Enforcement on October 6, 2006 – which is incorporated into the DOS-DHS MOA.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

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

Mitigation: This risk has been mitigated by ICE's practice of collecting only a limited amount of information about visa applicants from the source system, CCD, as is required to identify those applicants who warrant further investigation in the form of a visa security review. The CCD data extract contains a narrowly tailored subset of PII from the applicant's CCD record. ICE collects additional information about the applicant only if ICE selects the applicant for a more in-depth review, thereby limiting the amount of data collected in the system on the population of visa applicants as whole.

Privacy Risk: There is a privacy risk of compromise or improper use of PII associated with the creation and storage of multiple copies of applicant data on the local computers of VSP agents.

Mitigation: This risk is mitigated by ICE's policy of (1) providing secure computing environments and encrypting laptops and mobile hard drives, and (2) requiring VSP agents to delete locally stored files containing applicant data once a week.

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

Mitigation: ICE and the State Department personnel review the information collected about visa applicants during the visa security review before a final decision is made on the visa application. In addition, data accuracy will be further confirmed through biometric-based checks run by the State Department through the US-VISIT program, which compares biometrics of visa applicants against existing U.S. biometric databases. VSP checks against TECS and other databases will also help to identify potential inconsistencies or inaccuracies in the data, including attribution of data to the wrong individual, which can then be resolved by the VSP agent.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The information is used to identify U.S. visa applicants at high-risk locations abroad for further scrutiny before a visa decision is made. The information is also used by ICE to review and provide information to the State Department from DHS systems on applicants who are identified for a SAO. Information provided by the visa applicants is used to investigate those individuals to determine if there is adverse criminal, terrorism, immigration, or other information that may render them ineligible for a visa under Federal law. The results of the investigation are recorded in VSPTS-Net, including any information ICE conveys to the State Department. State Department officials use the information as part of their decision-making process whether to refuse or approve the visa.

The information is also used to manage and prioritize the workflow of VSP agents, and to track and manage performance metrics of the program. Information is shared with other VSP posts and with ICE Headquarters to facilitate visa security reviews, and oversight of the program.

2.2 What types of tools are used to analyze data and what type of data may be produced?

VSPTS-Net permits users to generate statistical reports, including number of visas screened, number of visas vetted, number of visas recommended for refusal, etc. In addition, VSP agents can use VSPTS-Net to create and save queries based on the security criteria used at a given post. VSP agents can also use the query tool as a filter to find all applicants that meet a certain security criteria, based on post-specific intelligence.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

VSP agents may use information from publicly available websites in the course of their investigations, but those systems will not interface with VSPTS-Net. VSP agents 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. Often this information is used to verify information provided by the visa applicant. VSP agents may at their discretion input information from publicly available websites into individual files.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.

In the standard operating procedures for VSPTS-Net and in the training provided to users, VSP agents and other system users are instructed how to protect information in the system from disclosure to inappropriate third parties. In addition, all ICE employees and contractors must take annual computer security and privacy training. Individuals who are found to have accessed or used the VSPTS-Net data in an unauthorized manner will be disciplined in accordance with ICE policy and federal law as appropriate. In addition, ICE conducts regular audits of VSPTS-Net users and maintains a thorough audit trail of all VSP activity.

The risk that VSPTS-Net information will be misused is mitigated by the fact that the only individuals that can access the information are ICE personnel (employees and contractors) that have a need to know in the performance of their official duties. Security and privacy training also mitigate the risk that sensitive information will be misused or handled improperly. The use of publicly available or commercial data presents a risk that ICE will rely on inaccurate information from these sources. This risk is mitigated by the collection and comparison of data from a variety of sources, including the visa applicant himself, during the visa security review. Inconsistent information will be identified and reconciled during this process.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Several different categories of records are retained: (1) visa applicant data extracts created from CCD (both the Excel and .txt file formats) and stored on the local drive for up to one week; (2) records of visa security reviews where ICE has no adverse finding and does not object to the issuance of a visa; (3) records of visa security reviews where ICE does not object to the issuance of a visa but provides derogatory information to the State Department regarding the applicant; (4) records of visa security reviews where ICE does not object to the issuance of a visa but provides terrorism-related information to the State Department regarding the applicant; (5) records of visa security reviews where ICE recommends against the issuance of a visa due to a nexus to terrorism; and (6) records of visa security reviews where ICE recommends against the issuance of a visa, with no nexus to terrorism.

3.2 How long is information retained?

ICE proposes to keep the categories of records described above for the periods identified below.

(1) Extracts of visa applicant data from CCD will be retained by ICE for no more than one week and then destroyed / deleted.

(2-3) Records of visa security reviews where ICE does not object to the issuance of a visa (including those where derogatory information is found and passed to the State Department) will be retained for 25 years after the date of review. This retention period will allow ICE to revisit VSP's transaction activity for key cases in which applicants had previously been reviewed and only later found to be potential matches for criminal or terrorist activity.

(4-5) ICE will retain for 75 years after the date of review records of visa security reviews where a) ICE does not object to the issuance of the visa but provides terrorism-related information to the State Department regarding the applicant, or b) ICE recommends 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.

(6) ICE will retain for 25 years records of visa security reviews where ICE recommends against the issuance of a visa where there is no nexus to terrorism. Given the ten-year statute of limitations on visa-related crimes, it is important for VSP agents 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 VSP agents to view previous casework on visas that are issued for ten-year multiple entry. VSP can also 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 ICE investigative efforts.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

No. ICE is drafting a retention schedule for its VSP records that will include the proposed retention periods described in Question 3.2 above.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

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 is retained for the timeframes outlined in Question 3.2 to ensure visa application information is available to ICE for an appropriate period to facilitate the processing of future visa requests for the same applicant, and for any future investigative efforts related to that applicant. This retention period is consistent with law enforcement system retention schedules generally and appropriate in length given the ICE's mission and the purpose of the Visa Security Program.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information used and stored in VSPTS-Net will be shared with other DHS components on an ad hoc basis as investigative needs arise, although ICE expects to share VSPTS-NET information primarily with CBP to support its border security mission.

4.2 How is the information transmitted or disclosed?

Information will be shared via telephone or email behind the DHS firewall, and by other secure transmission methods permitted under internal DHS policy for the handling and transmission of Sensitive Personally Identifiable Information (Sensitive PII). On an ad hoc basis, ICE may also input certain information from VSPTS-Net about a particular visa applicant directly into TECS by manually typing the information into a TECS record. Other users of TECS within DHS will thereby have access to the information.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: A risk is presented that information may be shared with DHS components without a need-to-know.

Mitigation: Information in VSPTS-Net is not routinely shared with other parts of DHS, and when it is shared, it is with components and officials that have a need for the information to perform their official duties such as CBP. VSPTS-Net is not accessible by users other than ICE personnel. Security and privacy training also mitigate the risk that sensitive information will be disclosed and handled improperly, or that information will be provided to other DHS components without a need-to-know.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ICE shares information about the results of its visa security reviews with State Department personnel to provide expert advice regarding specific security threats relating to the adjudication of the individual visa applications or class of application and a recommendation on whether to issue or deny the visa On an ad hoc basis, ICE also shares VSPTS-Net information with the appropriate Federal, State, local, or foreign organization responsible for investigating prosecuting, enforcing, or implementing, a statute, rule, or regulation where there is an indication of a violation of that statute, rule, or regulation.

ICE sharing of VSPTS-Net information outside of DHS that consists of or is derived solely from a State Department visa record is subject to confidentiality requirements under section 222(f) of the INA, and such sharing is further governed by the terms and conditions of the DOS-DHS MOA and the CA-ICE MOU.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes. The Visa Security Program Records SORN (DHS/ICE-012) provides routine uses that allow for the sharing of information described in Question 5.1 above. The sharing that is described is associated with the operation and mission of the Visa Security Program. In addition, the sharing of ICE data with the State Department is supported by the interagency sharing agreements cited above.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information may be transmitted either electronically or as printed materials to authorized personnel. All information is kept secure, accurate and controlled.

VSPTS-Net shares daily reports that contain expert advice regarding specific security threats relating to the adjudication of the individual visa applications or class of application and recommendation for the issuance of U.S. visas with the State Department. The reports are emailed to the appropriate State Department representative. Both the sender and receiver use State Department email addresses which enables greater security as the information remains within the State Department's network.

Regardless of agency, all Federal personnel at consular posts and embassies use State Department computers, networks and email, including ICE personnel. ICE determined that it would be more secure to use State Department email to send messages to the consular officers about visa security reviews, than using DHS email accounts which are on a different network. The need for using emails in support of VSP activities is temporary. Future upgrades to VSPTS will allow ICE to export its recommendations directly to CCD, at which time email will no longer be used.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: A risk is presented that information may be delivered to agencies outside of DHS that do not have a need to know VSPTS-Net information.

Mitigation: Information in VSPTS-Net is shared only with State Department officials that have a need-to-know the results of ICE's visa security reviews in order to make informed visa decisions that are in compliance with Federal law. VSPTS-Net information may also be shared for law enforcement or

intelligence reasons with agencies that have a need-to-know the information in the course of their official duties. Security and privacy training also mitigate the risk that sensitive information will be disclosed and handled improperly.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. The Visa Security Program Records SORN (DHS/ICE-012) and this PIA provide notice to the individual of the collection, intended use, and sharing of this information. In addition, the information provided by a visa applicant is considered a visa record subject to confidentiality requirements of INA section 222(f). The visa application form provides a confidentiality statement that the information collected is protected by section 222(f) of the INA which states that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Application for a U.S. visa is a voluntary action by a record subject. Individuals who voluntarily apply for a U.S. visa must supply all the requested information, and may not decline to provide part or all the information required, if they wish visa services.

A visa applicant may decline to provide information; however he/she is advised that this will result in a delay or denial of any visa services.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals who apply for a visa are put on notice that their information may be used as consistent with INA section 222(f). Visa applicants may decline to provide information; otherwise they have no right to consent to particular uses of the information or limit the use of the information.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: There is a risk of a lack of notice of the collection and uses of the information.

Mitigation: Visa applicants are provided three forms of notice about the use of their data in the VSP: this PIA, the Visa Security Program Records SORN, and the confidentiality notice included on the visa application form. These notices are accurate and reflect the current stated uses and sharing of the information. These notices are sufficient to mitigate any risks associated with a lack of notice of the collection of the information or the uses of the information. This notice is sufficient to mitigate any risks associated with a lack of notice of the collection of the information or the uses of the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals may request access to records about them in VSPTS-Net by following the procedures outlined in the Visa Security Program Records SORN. 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 individual access to records contained in VSPTS-Net could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal 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 the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

Additionally, information in a VSPTS-Net record that consists of or is solely derived from a State Department visa record is subject to the confidentiality requirements of INA section 222(f), which exempt particular information from being accessed and amended by the subject of the record.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). If an individual believes more than one DHS component maintains Privacy Act records concerning him or

her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If individuals obtain access to the information in VSPTS-NET pursuant to the procedures outlined in the Visa Security Program Records SORN, they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the Visa Security Program Records SORN. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Additionally, information in a VSPTS-Net record that consists of or is solely derived from a State Department visa record is subject to the confidentiality requirements of INA section 222(f), which exempt particular information from being accessed and amended by the subject of the record.

In addition to the procedures above, individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to:

ICE FOIA Officer
800 North Capitol Street, N.W.
5th Floor, Suite 585
Washington, D.C. 20528

Individuals may also submit requests by fax at 202-732-0310 or by email at ice-foia@dhs.gov. Please see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia/index.htm). If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

7.3 How are individuals notified of the procedures for correcting their information?

The procedure for submitting a request to correct information is outlined in the Visa Security Program Records SORN and in this PIA in Questions 7.1 and 7.2.

7.4 If no formal redress is provided, what alternatives are available to the individual?

As stated, individuals may submit Privacy Act requests for information and correction, which will be reviewed and corrected on a case-by-case basis.

As noted above, information in a VSPTS-Net record that consists of or is solely derived from a State Department visa record[4] is subject to the confidentiality requirements of INA section 222(f) which exempt particular information from being accessed and amended by the subject of the record.

Visa applicants may change their information at any time prior to submission of the application to the U.S Consulate or Embassy. Once a visa application is submitted, individuals may make changes only by filing a new application with the State Department or correcting the information during the course of a visa interview.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: A risk is presented that individuals are not aware of their ability to make record access requests for records in VSPTS-Net.

Mitigation: This risk is mitigated by the publication of this PIA and the Visa Security Program Records SORN, which describe how individuals can make access requests under the FOIA or Privacy Act. The nature of this system and the data it collects, processes and stores is such that the ability of individuals to access or correct their information may be limited for law enforcement reasons as expressly permitted by the Privacy Act. Permitting access to the records contained in VSPTS-Net could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal 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 the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies. However, outcomes are not predetermined and each request for access or correction is individually evaluated.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Only ICE personnel are granted user access to VSPTS-Net. Access to VSPTS-Net is role-based and is granted and limited by consideration of a user's need-to-know and mission responsibility. VSPTS-Net users will be divided into five categories: (1) VSP User, (2) SAO User, (3) Management-Level User, (4) Administrator, and (5) Headquarters User. To receive access to VSPTS-Net, a supervisor must submit a signed request recommending a user access level, based on the user's functional role, to determine the

[44] *See* State Department Privacy Act SORN State 39 - Visa Records, 60 FR 39469, August 2, 1995.

appropriate system privilege. The request is sent to the VSPTS-Net Administrator, where VSPTS-Net access may be granted or denied. The System Security Plan documents the system access policy for all user types listed below.

1) VSP Users - Review visa applications at VSP posts worldwide. VSP Users will have the ability to view, update, and make changes to applicant casework, and submit expert advice regarding specific security threats relating to the adjudication of the individual visa applications or class of application and a recommendation to State Department to issue or deny the visa. VSP Users can also view data from other VSP posts and the SAO Unit.

2) SAO Users - View, update and vet SAO applicant casework. SAO Users will then provide the State Department with expert advice regarding specific security threats relating to the adjudication of the individual visa applications or class of application and a recommendation to issue or deny the visa. SAO Users can also view data input from VSP posts.

3) Management-Level Users - Manage VSPTS-Net user accesses. They will grant or deny users access to make recommendations for other users and locations. Management-Level Users also have the ability to create queries for VSP and SAO users.

4) Administrators - Administrators, along with the Information Systems Security Officer (ISSO), will review each VSPTS-Net user account request to create the user account and manage the system maintenance. They are also responsible for periodically reviewing the user access list and disabling any user account that no longer requires access. 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.

5) Headquarters Users - Hold some exclusive privileges for reporting purposes. They will also have the ability to view and update applicant casework, and submit expert advice regarding specific security threats relating to the adjudication of the individual visa applications or class of application and a recommendation on visa issuance to the State Department.

8.2 Will Department contractors have access to the system?

Yes. ICE contract analysts in the SAO Unit and software developers have access to VSPTS-Net, subject to the same background, training, auditing, and confidentiality requirements as employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All ICE personnel and contractors complete annual mandatory privacy and security training and training on Securely Handling ICE Sensitive but Unclassified (SBU)/For Official Use Only (FOUO) Information. VSPTS-Net application training is provided by ICE OIA and includes guidance on appropriate uses of the system as well as issues relating to data accuracy.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The Certification and Accreditation process is in progress and is expected to be completed in September 2009.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

VSPTS-Net will use database-level auditing to capture user activity information associated with any viewing, insert, update, or deletion of records in the dataset, and the user that performed the activity. The VSPTS-Net application-specific audit trail provides adequately detailed information to facilitate reconstruction of events if compromise or malfunction occurs. The audit trail is protected from actions such as unauthorized access, modification, and destruction that would negate its forensic value. OIA reviews audit trails when there is indication of system misuse and at random to ensure users are accessing and updating visa records according to their job function and responsibilities during the pilot phase.

All failed logon attempts are recorded in an audit log and periodically reviewed. The VSPTS-Net ISSO will review audit trails at least once per week, or in accordance with the System Security Plan. The VSPTS-Net system and supporting infrastructure audit logs will be maintained as part of and in accordance with the existing ICE system maintenance policies and procedures for ICE.

ICE also has a process in place for investigating and responding to suspicious activities on the system. This process includes automated tools to assist the administrators in their monitoring, analysis, and reporting. The process is consistently followed. Additionally, VSPTS-Net runs within the DHS network and is protected by DHS network firewalls. There are no real-time interfaces between VSPTS-Net and other systems.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: The privacy risks to this system are the risks of unauthorized system access or use and inadequate system security.

Mitigation: Both risks have been mitigated by following DHS and government-wide security protocols that establish controls appropriate for this type of sensitive data. As described above and elsewhere in this PIA, those controls include user access controls, auditing, intrusion detection software, and user training.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

VSPTS-Net is a system modernization project, converting the original Microsoft Access application into one that is web-based.

9.2 What stage of development is the system in and what project development lifecycle was used?

VSPTS-Net is currently being developed with a target date of September 2009 to be operational.

9.3 Does the project employ technology, which may raise privacy concerns? If so, please discuss their implementation.

No.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security