

# Pre IVO Technology (piVot) Privacy Impact Assessment

## 1. Contact Information

### Department of State Privacy Coordinator

Sheryl Walter  
Bureau of Administration  
Global Information Services  
Office of Information Programs and Services

## 2. System Information

- a. **Date PIA was completed:** December 5, 2012
- b. **Name of system:** Pre IVO Technology
- c. **System acronym:** piVot
- d. **IT Asset Baseline (ITAB) number:** 6654
- e. **System description:**

The Pre IVO Technology (piVot) supports immigrant visa (IV) pre-processing at the National Visa Center (NVC) and Kentucky Consular Center (KCC), including IV case creation, IV package review, and support and inquiry functions. piVot interfaces with Consular Electronic Application Center (CEAC), electronic Document Processing (eDP), and Enterprise Queue Management (EQM) to achieve paper-less pre-processing for Immigrant Visa applications. When pre-processing is completed, piVot cases are transferred overseas for adjudication in the Immigrant Visa Overseas (IVO) system.

piVot is a custom developed HTML and PLSQL application available on OpenNet through the Consular Consolidated Database (CCD) Website. All piVot interfaces are brokered through CCD and Consular Affairs Enterprise Service Bus (ESB) services, including petition data ingest from partner agency, U.S. Citizenship and Immigration Services (USCIS) data shared status and messages for data collection through CEAC, and appointment scheduling in EQM.

f. **Reason for performing PIA:**

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

g. **Explanation of modification (if applicable):** N/A

h. **Date of previous PIA (if applicable):** N/A

## 3. Characterization of the Information

The system:

## Pre IVO Technology (piVot) Privacy Impact Assessment

- Does NOT contain PII. If this is the case, you must only complete Section 13.
- Does contain PII. If this is the case, you must complete the entire template.

**a. What elements of PII are collected and maintained by the system? What are the sources of the information?**

piVot collects and maintains identification of foreign nationals applying for immigration and contact information on U.S. persons (U.S. Citizens or Legal Permanent Resident (LPR) petitioners) and their legal representatives/agents. The sources of the information are systems collecting USCIS immigration petition data (via CLAIMS3) and Department of State immigrant visa application forms (via CEAC).

The elements are listed below, as collected for petitioners (U.S. Citizen or LPR) and applicant/derivatives (foreign nationals):

- Full Name (First, Middle, Last)
- Mailing Address
- E-mail address
- Telephone Number (Work, Home, Other)
- Date of Birth
- City of Birth
- Country of Birth
- Gender
- Marital Status
- Social Security Number (SSN)
- Alien Number
- U.S. Status
- Nationality
- Country of eligibility or chargeability for DV program
- Country where applicant is living
- Education level of applicant
- Number of children of applicant
- Income information for Joint Sponsors
- Tax ID
- Organization Name

piVot also interfaces with Electronic Document Processing (eDP) to review images of civil and financial documentation required as part of the IV application. The images themselves are not stored or maintained by piVot, but notes on their quality or condition will be stored by piVot. These images are collected through CEAC and stored in eDP or are scanned directly into eDP and viewed by piVot.

In the case of an applicant whose spouse or children are U.S. persons, the following PII is requested:

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

- Last name of applicant's spouse and children
- First names of applicant's spouse and children
- Middle names of applicant's spouse and children
- Dates of birth of applicant's spouse and children
- Genders of applicant's spouse and children
- Cities of birth of applicant's spouse and children
- Countries of birth of applicant's spouse and children
- Marriage information (dates of marriages, spouse full name, and place of marriage of past and present marriages)
- Digital color photographs of applicant's spouse and children

Additionally, if provided by the applicant or person preparing the entry on behalf of the applicant, the following optional PII on other U.S. persons may include:

- Last name
- First name
- Middle name
- Phone (Work)
- Phone (Home)
- Phone (Other)
- Email address

#### **b. How is the information collected?**

Petitioner and applicant PII is obtained from an individual petitioner who submits a petition (i.e., I-129, I-130, I-360, I-140, I-526, I-600, I-730, I-800/800A, I-824, or I-929) for immigration of the visa applicant to the USCIS. USCIS reviews and adjudicates the petition and forwards the approved petitions (presently in paper form) to Department of State NVC located in Portsmouth, NH for visa processing.

Some of the petitioner's data is transferred electronically to piVot via the CCD, which provides high performance secure connectivity between the Department of State and Department of Homeland Security (DHS) to support the exchange of visa data.

Updates to PII are submitted to the NVC and KCC in two ways: online or on paper. The petitioner, applicant or legal representative can complete the IV forms DS-230 (paper) or DS-260 (electronic through CEAC). Information may also be collected through telephone and email exchange. Public inquiry response agents will then update the applicant's records within piVot.

Diversity Visa applicants' PII is collected when the entrants file the DS-5501 Electronic Diversity Visa Entry Form (eDV Entry Form) available online at [www.dvlottery.state.gov](http://www.dvlottery.state.gov), which is transferred to the CCD and then to piVot. Supplemental information may also be collected on DVs through the DSP-122 form mailed to the KCC.

#### **c. Why is the information collected and maintained?**

Each element of PII collected and maintained by piVot is required by DHS USCIS to determine the eligibility of petitioner/applicants, to confirm the identities, to approve

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

immigrant visa applications, and for the Department of State to adjudicate the visa applications.

#### **d. How will the information be checked for accuracy?**

Accuracy of the information on an immigrant visa application is primarily the responsibility of the applicant or person filing the application on behalf of the applicant. Contract staff or Department personnel at NVC and Kentucky Consular Center (KCC) visually validate the authenticity and the completeness of the information received on the applicant from eDV, CEAC, DS-230, DS-260, and DSP-122 forms before transferring the case to post.

piVot's workflow includes quality check processes where critical data elements are confirmed as provided on the petition. Additionally certain fields are validated for accuracy through comparison of civil or financial documents submitted as part of the application process – for example, dates of birth and birth certificates, financial data and tax returns, and date of marriage, marital status, and marriage certificates.

#### **e. What specific legal authorities, arrangements, and/or agreements define the collection of information?**

piVot was developed to support U.S. immigration and nationality law as defined in the major legislation listed below:

- Immigration and Nationality Act (INA) of 1952, 8 U.S.C. 1101, et al. (as amended)
- INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- 22 U.S.C. 2651(a) (Organization of Department of State)
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Child Status Protection Act of 2002 ( P.L. 107-208)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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

The collection of PII creates the vulnerability that DHS USCIS and the Department of State – NVC/KCC employees may use the PII for purposes other than those required by the Department of State and thereby misuse the PII. The potential threats to privacy include:

- Inadequate security by the USCIS and Department of State — USCIS and Department of State employees may create a new repository of PII that is vulnerable to unauthorized access, use, disclosure and retention;

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

- Inadequate data integrity — USCIS and Department of State data entry personnel may enter the data into piVot wrong and may modify the data without authorization; and
- Inadequate openness and transparency — USCIS may not provide sufficient details to allow applicants to understand how their information will be used.

As it relates to immigrant visa processing, the impact of these threats to the applicants could include delays in responses, possible subsequent denial of immigration to the United States based on faulty data, or misuse of PII. As it relates to USCIS and the Department of State collection of PII, the impact of these threats to the applicant can include the loss of control over the use and disclosure of their PII. The opportunities for the misuse of PII, the serious impact that misuse would have to covered petitioners, and the integrity of the piVot makes the misuse of PII by USCIS and the Department of State a serious risk.

DHS and the Department of State seek to address these risks by limiting the collection and transmission of PII to the information required to execute these processes. Moreover, only authorized users with a need to know are granted access to piVot.

#### **4. Uses of the Information**

##### **a. Describe all uses of the information.**

The information collected by piVot is used for processing, auditing and tracking of individual immigration visa applications as well as tracking the number of immigrant visas assigned that are subject to numerical limitations based upon the visa classification and country of chargeability.

In actual practice the main element used to retrieve case records is the Case ID assigned by piVot; however, records may also be retrieved by querying the last name, first name, or date of birth for persons related to a case (such as the petitioner, principal applicant, or derivatives).

##### **b. What types of methods are used to analyze the data? What new information may be produced?**

A series of transactional reports are used to analyze workflow data through case processing. Fraud Prevention Units at NVC and KCC also may perform additional analysis based on fraud indicators. New information produced through fraud analysis may include memoranda that Posts may utilize to recommend USCIS revoke immigrant petitions, or data to capture fraud research within the Enterprise Case Assessment Service (ECAS) tool.

Human review of the completeness and quality of the submitted IV Package (Fees, Forms, and Documents) is a major piVot workflow function. During this review, users analyze the correctness and completeness of case data by viewing submitted data forms or images from submitted documents. Based on the results of this review, new information in the form of comments to correct what was submitted is produced and shared back to the applicant/petitioner/attorney through CEAC or written

## **Pre IVO Technology (piVot) Privacy Impact Assessment**

correspondence. New information in the form of case notes for overseas processors and adjudicators may also be produced and transferred with the case to IVO.

- c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.**

USCIS petition data from the CLAIMS3 system serves as the basis for all immigrant visa cases. This data is used to create the piVot case. Once created, piVot uses data collected through CEAC to review the completeness and quality of the submitted IV Package (Fees, Forms, and Documents). No other commercial information, publicly available information or information from other Federal agency databases is used.

- d. Are contractors involved in the uses of the PII?**

Yes, the majority of piVot users are contractors staffing the operations of NVC and KCC. Terms of employment for all contractors include a SECRET clearance and Privacy Act information clauses. Further, contractors are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

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

All piVot user activity is tracked and audited at the database level. Further the application performs basic internal validations on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

All users, including external agency users, are screened prior to their employment with the Department of State or with their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Each domestic organization has at least one Security Officer who is responsible for managing the users within the organization. Security Officers are government employees who approve account requests and determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Contractors who support piVot are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual.

## **Pre IVO Technology (piVot) Privacy Impact Assessment**

At the very minimum, contractors involved in the development and/or maintenance of piVot hardware and software must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing the piVot.

In addition, before they are given access to the OpenNet and any CA/CST system, including piVot, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

It is mandatory for all Department of State employees and contractors to complete an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer.

The CA post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified (SBU) data from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the posts, domestic sites, and external agencies for the proper disposal of paper that is SBU.

All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

### **5. Retention**

#### **a. How long is information retained?**

The retention time of the visa records varies depending upon the specific kind of record. Files of closed cases are retired or destroyed in accordance to the published record schedules of the Department of State and the National Archives and Records Administration, specifically [General Records Schedule 20 items 2b and 2c](#). Some records, such as refused records, are retained until the subject is 100 years old and 10 years have passed since the last visa activity. Procedures are documented at the Office of Freedom of Information, Privacy, and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

#### **b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.**

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.

The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of piVot throughout the lifetime of the data. Accuracy of the data is verified as described in section 3(d) above. The information is only retained for the amount of time that is required to perform the System's purpose.

## Pre IVO Technology (piVot)

### Privacy Impact Assessment

Department of State OpenNet security protocols are used to ensure that the data is stored and backed up in a secure environment. Regular backups are performed and recovery procedures are in place for piVot.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

#### 6. Internal Sharing and Disclosure

- a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

System Name and Acronym	Manner of sharing	Type of data and how it is shared
<b>Electronic Diversity Visa (eDV)</b>	One-way: From piVot to eDV/ESC	The eDV system checks the Packet 3 (Information Letter) and Packet 4 (Interview Letter) tables in DVIS for new data. The P3 data is uploaded to the eDV/ESC system where status and letters are available for applicants. Later on in the DV process, the P4 data is uploaded to the eDV/ESC system where instructions and appointment information are available for DV winners.
<b>Consular Consolidated Database (CCD)</b>	Two-way	piVot connects to CCD for production data replication.
<b>Immigrant Visa Allocation and Management System (IVAMS)</b>	Two-way	piVot receives the statistical data and allocation information in the form of a text file from IVAMS via OpenNet email and DVIS uses the information to process Diversity immigrant visas. piVot emails the Monthly Report of Qualified Visa Applicants in the form of a text file to IVAMS. Three other reports from DVIS are faxed from KCC to the Visa Office for updates to IVAMS.
<b>Immigrant Visa Information System (IVIS)</b>	One-way	Legacy IV case records to be migrated to piVot.
<b>Immigrant Visa Overseas (IVO)</b>	One-way: From piVot to IVO	piVot transfers immigration cases to IVO for final processing.

**Pre IVO Technology (piVot)  
Privacy Impact Assessment**

<b>System Name and Acronym</b>	<b>Manner of sharing</b>	<b>Type of data and how it is shared</b>
<b>Consular Electronic Application Center (CEAC)</b>	Two-way	The CEAC system interacts with the applicant/petitioner/attorney while DoS is processing their visa application. It is the vehicle to collect for immigrant visa fees, application data, and imaged civil documents. It is also the system which communicates feedback and processing results including notes made during the IV Package Quality Review in piVot.
<b>Electronic Document Processing (EDP)</b>	One-way From EDP to piVot	The EDP system is used to scan/image paper documents received by NVC and KCC. It is also the system which stores images collected through CEAC. While a case is being processed piVot views those stored images in EDP but does not add any data to EDP.
<b>Enterprise Queue Management (EQM)</b>	Two-way	The EQM system provides CST with Enterprise Calendaring and Appointment management. As cases are ready to be scheduled for an overseas appointment piVot sends the case to EQM. EQM then schedules the case into a given appointment slot and returns the scheduled data to piVot.
<b>Enterprise Case Assessment Service (ECAS)</b>	Two-way	ECAS provides DoS Fraud Prevention Units a tool to track and record results of fraud investigations. If a piVot user suspects fraud, they will refer the case to ECAS where research is stored. When the results of the research are completed as final fraud findings ECAS shall provide an update to the piVot case through inserting a case note.

**b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?**

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. An Interface Control Document (ICD) and/or Memorandum of Understanding (MOU) define and disclose transmission format via OpenNet. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords, and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

**c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.**

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. piVot mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements.

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

Vulnerabilities and risks are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

Access to information is controlled by application access controls. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department of State regulations.

piVot has formal, documented procedures to facilitate the implementation of its audit and accountability processes. The application produces audit records that contain sufficient information to establish what events occurred, the sources of the events identified by type, location, or subject. System administrators regularly review and analyze the application audit records for indications of suspicious activity or suspected violations of security protocols.

## **7. External Sharing and Disclosure**

### **a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?**

USCIS shares information collected on immigrant visa petitions with the Department of State for the purpose of establishing the basis for the beneficiaries of the immigrant visa petitions to submit immigrant visa applications to the Department of State. The Department of State does not share information with external organizations other than DHS USCIS directly from piVot.

### **b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?**

Information shared outside the Department is exchanged through the Consular Consolidated Database (CCD), and uses all safeguards in place by the CCD to maintain security through external data exchanges.

In all cases of sharing with DHS, all components are required to comply with the Department's security policies and procedures, particularly the DHS Information Technology (IT) Security Program Handbook for Sensitive Systems (Attachment A to DHS Management Directive 4300.1). This handbook establishes a comprehensive program for DHS to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules, which are applied to component systems, communications between component systems, and at all interfaces between component systems and external systems.

Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a Memorandum of Understanding (MOU) or exchange of letters as well as technical documentation including an Interface Control Document (ICD) and Interconnection Security Agreement (ISA). Data is sent through encrypted lines.

### **c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.**

## Pre IVO Technology (piVot) Privacy Impact Assessment

Any data sharing, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. piVot mitigates these vulnerabilities by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data. The security program involves the establishment of strict rules of behavior for each major application, including piVot. It includes a periodic assessment of physical, technical, and administrative controls designed to enhance accountability and data integrity. It also requires that all users be adequately trained regarding the security of piVot, that system users must participate in a security training program, and that contractors and consultants must also sign a non-disclosure agreement. External connections must be documented and approved with both parties' signature in an ISA, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

### 8. Notice

The system:

- Contains information covered by the Privacy Act.  
Provide number and name of each applicable system of records.  
(visit [www.state.gov/m/a/ips/c25533.htm](http://www.state.gov/m/a/ips/c25533.htm) for list of all published systems)
- Visa Records. STATE-39
- Does NOT contain information covered by the Privacy Act.

#### a. Is notice provided to the individual prior to collection of their information?

Although piVot does not collect information directly from persons, the various USCIS forms (I-130, I-140, I-129F, I-360, I-536, I-600, I-600A, I-824, I-800) do provide notice explaining the reason for collecting PII for IV processing, how it will be used, and the effect of not providing the PII. Refer to the USCIS website, <http://www.uscis.gov/portal/site/uscis>, for more details on the USCIS forms.

Department of State data collection is performed through either CEAC or the Electronic Diversity Visa (eDV) Applicant Entry System (AES). Both web data-collection tools provide a statement that the information collected is protected by section 222(f) of the Immigration and Nationality Act (INA). INA section 222(f) provides 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.

Also, notice is provided in the System of Records Notice Visa Records, State-39.

#### b. Do individuals have the opportunity and/or right to decline to provide information?

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

Yes, the petitioners have the right to decline to provide PII for use in processing their immigration visa application. However, failure to provide the information necessary to process the application may result in the application being rejected.

Information is given voluntarily by the applicants and with their consent, by a legal representative or other person.

Individuals who voluntarily apply for a U.S. immigration visa must supply all the requested information, and may not decline to provide part or all of the information required if they wish to receive an immigrant visa.

**c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?**

Information is given voluntarily by the applicants or his/her representative. No other special uses of the information are permitted. Individuals are advised on the use of the information being collected at the time of collection.

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

For IV petitioners, piVot relies on State-39 and on the notice given to the petitioners who fill out the form to mitigate the privacy risks posed by collection and use of PII. Additional notice is provided directly in CEAC and eDV-AES when collecting applicant data.

The mechanisms for notice offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the INA. The information provided on the immigrant visa forms and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

Access to piVot is restricted to cleared, authorized Department of State direct hires and contractor personnel. piVot enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

## **9. Notification and Redress**

**a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?**

Information in piVot is considered a visa record subject to confidentiality requirements under INA 222(f). piVot information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a). In addition, covered petitioners may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

## **Pre IVO Technology (piVot) Privacy Impact Assessment**

IV applicants may change their information anytime during processing of a piVot case. The IV applicant may submit updates to contact information in the form of email addressed through CEAC. Up until the full IV package and application are submitted, the IV applicant may submit updated information through CEAC or by contacting the NVC or KCC by telephone or email. Processing Specialists at NVC and KCC will update case data at the request of the IV applicant. Processing Specialists at NVC and KCC may also identify discrepancies and send messages through CEAC requesting updated or corrected information. These corrections are made directly in CEAC and transferred back to piVot through the CCD.

Once an application has been submitted applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request in addition to case status information, and this guidance is available to the public in 9 FAM 40.4:

- (1) Correspondence previously sent to or given to the applicant by the post;
- (2) Civil documents presented by the applicant and
- (3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.32 informing the individual how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.36.

### **b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.**

To the extent information in piVot may be covered under the Privacy Act, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in piVot.

## **10. Controls on Access**

### **a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

Internal access to piVot is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. To access the

## **Pre IVO Technology (piVot)**

### **Privacy Impact Assessment**

system, persons must be authorized users of the Department of State's unclassified network. Access to piVot requires a unique user account assigned by a supervisor.

The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

**b. What privacy orientation or training for the system is provided authorized users?**

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training. Additionally, all Federal employees must take PA-459, a course entitled Protecting Personally Identifiable Information.

Internal based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

**c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.**

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Therefore, this level of privacy risk is negligible.

Additionally, system audit trails are available to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform--or may attempt to perform. As a result of these actions, the residual risk is low.

## **11. Technologies**

**Pre IVO Technology (piVot)**  
**Privacy Impact Assessment**

**a. What technologies are used in the system that involves privacy risk?**

piVot does not employ any technology known to elevate privacy risk.

**b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

Since piVot does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

**12. Security**

**a. What is the security certification and accreditation (C&A) status of the system?**

The Department of State operates piVot in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State is conducting a risk assessment of the system to identify appropriate security controls to protect against risk and has implemented security controls. The Department of State will perform routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision, piVot is currently undergoing its initial Certification and Authorization (C&A) and is expected to be authorized in December of 2012.