



**Privacy Impact Assessment (PIA)**

**For: Immigrant Visa Overseas**

**Version 04.07.03**

**Last Updated: June 25, 2015**

## 1. Contact Information

|   |
|---|
| <b>A/GIS/IPS Director</b><br>Bureau of Administration<br>Global Information Services<br>Office of Information Programs and Services |
|---|

## 2. System Information

- a. **Date PIA was completed:** June 25, 2015
- b. **Name of system:** Immigrant Visa Overseas
- c. **System acronym:** IVO
- d. **IT Asset Baseline (ITAB) number:** # 817
- e. **System description (Briefly describe scope, purpose, and major functions):**

IVO provides automated support to the adjudication of an immigrant or a diversity visa application from individuals wishing to come to the United States with the intent to establish permanent residence. IVO also provides for the administration of federal law and regulations that govern the issuance or refusal of either visa type. IVO is a case record and maintenance application used at overseas posts to review and complete the visa adjudication. IVO's main processes are:

- Immigrant visa (IV) case processing, name clearance (through interfaces with name check applications), fingerprint and facial recognition clearance (through interfaces with biometric applications), adjudication, visa issuance, and refusal recording and tracking;
- Visa allocation management for allocations assigned to post;
- Biometric data collection (such as fingerprints and images for facial recognition);
- Automated tracking, scheduling and reporting of applicant interviews and medical exams;
- Internal fraud control, workload statistic management for post and Fraud Prevention Program managers; and
- Waiver processing.

**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):** 07/09/2010

### 3. Characterization of the Information

The system:

- 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?**

IVO primarily collects data on foreign nationals as part of the U.S. immigrant visa application process. As such, the information provided by the immigrant visa applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA). Because immigrant visa applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not currently covered by the provisions of the Privacy Act or E-Government Act of 2002. However, IVO records may include PII about persons associated with the applicant who are U.S. citizens or legal permanent residents. This PII data may include the following: U.S. sponsor's name; date of birth; place of birth; telephone numbers; address; gender; language used; relationships; occupation; employment information; employer information; financial information; aliases; biometric data; alien registration number; marital status; nationality; final U.S. address; passport number and other passport issuance information; national identification; arrival date; and duration of stay information. In any given case the data stored can vary. The variation is dependent on what data was input into the case at inception.

The source of information is the subject of the record, relatives, such as parents, sponsors, and attorneys/agents representing applicants.

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

The information is collected by consular posts from visa applications, passports, corroborating documentation and in-person interviews. Some of the case data is electronically transferred from the Immigrant Visa Information System (IVIS) used domestically by the National Visa Center (NVC) or Diversity Visa Information System (DVIS) used domestically by the Kentucky Consular Center (KCC) applications, which are used to process imported data or input additional information and from approved immigrant visa petitions (filed by U.S. citizens with the Department of Homeland Security's U. S. Citizenship and Immigration Service (DHS/USCIS).

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

The information is collected to determine the eligibility of foreign nationals who have applied or are applying for an immigrant or diversity visa to immigrate to the United States.

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

Accuracy of the information on an immigrant visa application is the responsibility of the applicant and IVO users including the Department of State employees and contractors working domestically and overseas. In addition, quality checks are conducted against the submitted documentation at every stage, and administrative policies minimize instances of inaccurate data.

Locally Engaged (LE) staff at post will review the initial documentation and identification forms in the hard file sent by NVC against what is loaded into the IVO application from IVIS. Any new documentation or identification forms submitted by the applicant from that point onward are also reviewed and verified against data in IVO. IVO also allows users to conduct and annotate the results of any local and/or governmental background and identity checks. Any changes to biographical data thereafter will alert the users that new checks need to be performed. In some instances the IVO application will detect changes and will then initiate an automated check without user intervention. The final stage of review is the interview and final adjudication conducted by a Foreign Service Officer (FSO). The FSO will verify that all information is factually correct before adjudicating the visa.

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

The following authorities provide for the administration of the program supported by IVO:

- Immigration and Nationality Act of 1952 (INA) (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- 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 personal data collected by IVO is the minimum necessary to carry out the function of IVO as identified in Section 3(c) above.

Risk factors are mitigated through the use of Technical, Management, and Operational security controls. The IVO application data is protected by multiple layers of security controls including OpenNet (the Department's internal unclassified network/intranet) security, IVO application security, Department site physical security and management security.

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

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

IVO is used by consular officers to record information for name checks, fingerprint matching, and other searches to verify the identity of the applicant and to help determine if the applicant is eligible for travel and immigration to the United States under applicable immigration laws and regulations. Consular officers use the information to make a determination whether to grant an Immigrant Visa (IV).

Data can be retrieved in IVO by keyword searches such as applicant name, alien registration number, case number, and/or by barcode scanning.

Issuance and refusal information is shared with the Department of Homeland Security (DHS) including name, date of birth, gender, and visa information such as issuance or refusal date and visa foil number.

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

IVO generates a variety of reports for statistical and management purposes. These include:

- Accountability reports that contain detailed information on a specified case and its applicants such as The Case Accountability Report.
- Management reports that are reviewed by consular management for unusual and inexplicable activity such as: Critical Fields Changed In Case/Applicant, Cases Deleted, Potential Duplicate Cases/Applicants, Outstanding FBI Clearance Applicants and Visas Returned and Not Reissued.
- Standard reports such as: Monthly Report of Qualified Visa Applicants (FS469), Returned Visa Authorizations, Daily Appointment Schedule, Monthly Immigrant Visa Workload, Annual Report of Active Visa Applicants and Annual Report of Inactive Visa Applicants.
- Query reports such as: Recalled Cases, Refused Applicants, Applicants Subject To Numerical Limitations Eligible For Appointments, Applicants Not Subject To Numerical Limitations Eligible For Appointments, Adjudicated Special Interest Cases, Applicants With Overcome/Waived Refusals and OF230 P1 Namecheck Hits.

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

Namecheck requests are routed through the Bureau of Consular Affairs' (CA) CLASS database, which contains lookout information provided from the Drug Enforcement Administration (DEA), the Department of Homeland Security (DHS), the Department of Health and Human Services (HHS), the Federal Bureau of Investigation (FBI), and Interpol.

Fingerprint checks are routed through the FBI's Integrated Automated Fingerprint Identification System (IAFIS), as well as DHS' Integrated Biometric System (IBS) database.

Under the Hague Convention on Protection of Children and Co-operation in Respect of Inter-country Adoption, the Department of State, Office of Children's Issues is responsible for monitoring and overseeing the accreditation or approval of adoption service providers that want to perform adoption services with other countries that are party to the Convention. The names of accredited or approved Adoption Service Providers are then forwarded to post to be used in a drop down field in IVO for the user to select.

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

IVO is a government-owned system. It is supported by contract employees, some of whom are located at contractor-owned facilities. No contractors are involved in using the PII to carry out the function of IVO as identified in Section 3(c) above. Direct hire U.S. government employees have the sole responsibility for processing IV case data in IVO and adjudicating IV applications to determine if applicants are entitled to IV issuance.

**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.**

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit restriction of categories of information and reports. Consular managers 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. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the IVO application. Mandatory annual security/privacy training is required for all authorized users including regular refresher training.

All users are screened prior to their employment with the Department. 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. In addition, before being given access to the OpenNet and any CA/CST systems, including IVO, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Consular post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard PII from unauthorized disclosure by storing printed or electronic media containing PII in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that contains PII.

Contractors involved in the design, development, and maintenance of IVO are required to have a Moderate Risk Public Trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and Homeland Security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of IVO hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

## **5. Retention**

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

Record retention varies depending upon the type of records. Files of closed cases are disposed in accordance with published Department of State record schedules as approved by the National Archives and Records Administration (NARA).

These are the records schedules pertaining to IVO:

**B-09-002-08a Immigrant Visa Overseas (IVO) System - Issuances**

Description: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Disposition: TEMPORARY. Cutoff at end of calendar year when issued. Destroy 5 years after cutoff or when no longer needed, whichever is sooner.

DispAuthNo: N1-084-09-02, item 8a

**B-09-002-08b Immigrant Visa Overseas (IVO) System - Cat I Refusals**

Description: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Disposition: TEMPORARY. Cutoff at end of calendar year when refused. Destroy 100 years after cutoff or when no longer needed, whichever is sooner.

DispAuthNo: N1-084-09-02, item 8b

**B-09-002-08c Immigrant Visa Overseas (IVO) System - Cat II Refusals**

Description: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Disposition: TEMPORARY. Cutoff at end of calendar year when refused. Destroy 25 years after cutoff or when no longer needed, whichever is sooner.

DispAuthNo: N1-084-09-02, item 8c

**B-09-002-08d Immigrant Visa Overseas (IVO) System - Abandoned Cases**

Description: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Disposition: TEMPORARY. Cutoff at end of calendar year when abandoned. Destroy 50 years after cutoff or when no longer needed, whichever is sooner.  
 DispAuthNo: N1-084-09-02, item 8d

**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 the records exist, the more likely inaccuracies will develop as a consequence of aging.

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. 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 National Archives 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?**

IVO information is shared with authorized Department of State consular officers and staff that may be adjudicating a visa case or handling a legal, technical or procedural question resulting from an application for a U.S. visa. Application case data, previous case history, adoption information, visa allocations, issuance and refusal statistics, workload statistics and lookout data are shared internally to perform immigrant visa functions and services.

The following internal Department of State system(s) are connected electronically and share the following information: U.S. sponsor's name, date of birth, place of birth, telephone numbers, address, gender, language used, relationships, occupation, employment information, employer information, financial information, aliases, biometric data, alien registration number, marital status, nationality, final U.S. address, passport number and other passport issuance information, national identification, arrival date, and duration of stay information.

| #  | System Name and Acronym                     | Type of Data  |
|----|---|---|
| 1. | Consular Lookout And Support System (CLASS) | Applicant name check: confirmation that no aliases are present and verification of supplied information. It is used by passport agencies, consulates, and border inspection agencies to perform name checks on visa and passport applicants in support of the issuance process. Queries to CLASS contain information such as the name, data of birth, |

| #  | System Name and Acronym                             | Type of Data  |
|----|---|---|
|    |   | and place of birth. These data elements are used to determine entries in the CLASS database that are, or could be, the subject of the query.  |
| 2. | Non-Immigrant Visa System (NIV)                     | Transfer of cases   |
| 3. | Independent Namecheck (INK)                         | The Independent Namecheck (INK) application provides the capability to conduct namecheck queries and add lookouts to CLASS for individuals who are not applying for a visa. The INK query function replaces the independent namecheck query function that was part of the IVO system.   |
| 4. | Immigrant Visa Information System (IVIS)            | Transfer of cases   |
| 5. | Diversity Immigrant Visa Information System (DVIS)  | Transfer of cases   |
| 6. | Immigrant Visa Allocation Management System (IVAMS) | Visa allocation management  |
| 7. | Accountable Items (AI)                              | The Accountable Items module tracks and controls the valuable visa foils and passport forms.  |
| 8. | Ten Print Live Scan System (TPLS)                   | Ten-Print Live scan (TPLS) performs the fingerprint capture and quality scoring and stores fingerprints in the database. IVO calls TPLS and passes it the IVO case number for which a fingerprint capture needs to occur. TPLS returns the fingerprint scores and indicates if capture was successful. TPLS is also used to perform fingerprint verification and to display images of previously captured fingerprints. |

**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 under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet. The Department of State systems that interface with the IVO are strictly controlled by

firewall and network intrusion detection systems (NIDS) rules that limit ingress and egress to the IVO. All changes are requested from the Firewall Advisor Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented.

All physical records are maintained in secured file cabinets or in restricted areas to which access is limited to authorized personnel and contractors. Access to electronic data is protected by passwords and is directly under the supervision of system managers.

The following safeguards are in place for each sharing arrangement:

- 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.
- Additionally, audit trails monitor computer usage and access to files.
- Finally, regularly administered security/privacy training informs authorized users of the proper handling of data, privacy, and security issues.

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

The aforementioned PII contained in IVO is shared solely within the Bureau of Consular Affairs among cleared employees with role-based access to the data via secure transmission methods. As such, the privacy risk from internal sharing is negligible.

## **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?**

The IVO data: applicant biometric data (fingerprints, photo), personal data, and issuance data are shared with other federal agencies via Consular Consolidated Database (CCD) data sharing arrangements for the following purposes:

- Checking the applicant's fingerprint information against Department of Homeland Security (DHS) databases
- Establishing a record within DHS' Integrated Biometric System (IBS)
- Use at U.S. ports of entry to verify the validity of the visa
- Checking to determine if the person has a criminal record that would have an effect on visa eligibility

Since the sharing of this information is not a direct external interconnection to IVO, this PIA does not provide technical details regarding data sharing and protection.

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

IVO data is replicated from the databases at each post to the CCD. When the CCD receives fingerprint requests or visa issuance data, the CCD forwards the information to the Department's datashare applications.

Each datasharing arrangement with federal agency partners is covered by a written agreement in the form of a Memorandum of Understanding or exchange of letters as well as technical documentation, including an interface control document and interagency security agreement. Data transmissions are encrypted.

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

IVO information is shared with U.S. government agencies pursuant to statute and is in accordance with confidentiality requirements under INA section 222(f). Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly followed in order to ensure that any risk is addressed through the user-authorization process.

**8. Notice**

The IVO system:

- contains information covered by the Privacy Act.  
Provide number and name of each applicable system of records notice.  
Visa Records – STATE-39  
Overseas Citizens Services Records – STATE-05
- does NOT contain information covered by the Privacy Act.

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

The application forms explain the reason for the information collection, how the information will be used, and potential outcome of not providing information. A list of forms an applicant might use is:

- DS-260 (electronic immigrant visa form) or DS-230 Parts I and II: Application for Immigrant Visa and Alien Registration – the Department of State's main application form for all immigrant visa applicants.

For adoption purposes, the adoptive parents will submit the following Department of Homeland Security forms.

- I-600: Petition to Classify Orphan as an Immediate Relative (Non Hague).
- I-600A: Application for Advance Processing of Orphan Petition (Non Hague).
- I-604: Determination on Child for Adoption (Non Hague).
- I-800: Petition for a Hague Child (Hague approved)
- I-800A: Application for Determination of Suitability to Adopt a Child from a Convention Country

The application forms provide a statement that the information collected is protected by section 222(f) of the Immigration and Nationality Act of 1952, as amended (INA). INA section 222(f), 8 U.S.C. 1202(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.

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

Information is given voluntarily by the consenting applicants, by family members and other designated agents. Failure to provide the information necessary to process the application may result in the application being rejected.

**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.**

IVO relies on the notice given to the applicants who fill out the form to mitigate the privacy risks posed by collection and use of PII.

The notification and redress mechanisms 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 form and in the System of Records Notice (SORN) regarding visa records, STATE-39, fully explains how the information may be used by the Department and how it is protected.

Access to IVO is restricted to cleared, authorized Department of State direct hires and contractor personnel. IVO 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?**

Visa applicants may change their information at any time prior to submission of the application to the U.S. Consulate or Embassy. Once that is done, 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, 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.

IVO information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to and/or correction of their PII pursuant to the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate.

Procedures for requesting access to and/or correction of records are published in Title 22 of the Code of Federal Regulations Section 171.( 22 CFR 171.) Certain exemptions to Privacy Act provisions for access to and correction of records may exist for visa records on law enforcement grounds, 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.

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

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

## **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?**

Access to IVO requires a unique user account assigned by a supervisor, and is limited to authorized Department of State users, including contractors that have a justified need for the information in order to perform official duties. To access the system, an individual must be an authorized user of the Department of State's unclassified network (OpenNet). Each authorized OpenNet user must sign a user access agreement before receiving 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. The level of IVO 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 reiterates the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists restrict categories of information and reports. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the IVO application. Mandatory annual security/privacy training is required for all authorized users including regular refresher training.

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

The Department requires all direct-hire employees who handle personally identifiable information (PII) while performing their official duties to satisfactorily complete the Foreign Service Institute (FSI) distance learning course PA459, Protecting Personally Identifiable Information (PII).

Additionally, all Department employees must take and pass an annual Cyber Security Awareness Training course, which includes elements of privacy training, in order to retain access to the Department's unclassified network, which is a prerequisite to accessing IVO. Furthermore, IVO users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

**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.**

CA has implemented comprehensive controls to limit access to this system and regulate the behavior of authorized users of IVO. Expected residual risks related to access are negligible.

## 11. Technologies

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

IVO is a government off-the-shelf (GOTS) product that meets required security capabilities, approved design and development processes, required test and evaluation procedures and documentation under the supervision of a Project Manager in accordance with Department of State internal policy. Additionally, IVO receives input from Department of State security officers regarding any potential security issues.

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

Since IVO does not use any technology known to elevate privacy risk, the current, implemented IVO safeguards are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

## 12. Security

**a. What is the security assessment and authorization (A&A) status of the system?**

The Department of State operates IVO in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls on a regular basis to ensure that the controls continue to function properly. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the assessment and authorization of IVO is expected to be completed by December 2015. This document was updated as part of the reauthorization of the system.