Privacy Impact Assessment (PIA): Immigrant Visa Overseas System (IVO)

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: 07/09/2010

(b) Name of system: Immigrant Visa Overseas System (IVO)

(c) System acronym: IVO

(d) IT Asset Baseline (ITAB) number: 817

(e) System description:

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;
- 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 re-certification

☐ PIA Information Review

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

(h) Date of previous PIA (if applicable): 12/1/2008

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 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; 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.

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 oversees from visa applications, passports, corroborating documentation and in-person interviews.

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 a visa to travel 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/contractors/customer service reps/consular officers overseas.

In addition, quality checks are conducted against the submitted documentation at every stage, and administrative policies minimize instances of inaccurate data. Foreign Service Nationals (FSN) will review the initial documentation and identification forms in the hard file sent by the National Visa Center (NVC) against what is loaded into the IVO application. 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 correct and factual before issuing the visa.

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

- Immigration and Nationality Act (INA) of 1952 (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.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are:

- **Device theft or loss-** Lost or stolen laptops and other devices such as removable drives may contain PII.

- **Portable Devices-** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players creates risk by making PII easily transportable on devices that aren't always properly secured.

- **Insider threat-** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest

- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the information assurance standards published by the National Institute of Standards and Technology (NIST), there are management, operational, and technical security controls implemented to protect the data. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), training, and audit reports.

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 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, DOB, 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 the Immigrant Visa Overseas (IVO) officer 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.

Visa applicant data such as photo, fingerprint, proof of birth, birth place, other identifying documents, existing passports provided by visa applicants and/or foreign authorities is used to effectively identify the visa applicant and determine eligibility to immigrate to the United States.

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 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. Is the system a contractor used and owned system?

IVO is a government-owned system. It is supported by contract employees, some of whom are located at contractor-owned facilities. Direct hire U.S. government employees have the sole responsibility for adjudicating IV applications to determine if applicants are entitled for IV issuance.

All employees and contractors must pass an annual cyber computer awareness training course and are briefed on their responsibilities under the Privacy Act when handling personally identifiable information (PII). All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

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 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. 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 security training and regular refreshment training.

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

Consular officers/users, system administrators, and database administrators are trained through the annual cyber security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts 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.

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).

Some records/cases are kept on file for the purpose of determining eligibility as opposed to a data requirement. For example, records of applicants who failed to make an appointment are deleted after three years, while lookout records are retained until the subject is 100 years old and 10 years have passed since the last visa activity.

Paper records produced by this application are shredded or burned, per internal Department of State requirements for handling visas and Department of State record disposition schedules.

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.

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 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?

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 owned by the same system owner of IVO; however, they are outside of the IVO accreditation boundary. They fall under the purview of the Department's Designated Approval Authority; hence, CA does not require Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), or Service Level Agreement (SLA) for CA owned systems connected to IVO via OpenNet. Controls built in the OpenNet GSS, including Firewalls and Network Intrusion Detection Systems (NIDS) provide network level controls that limit the risk of unauthorized access.

Shared System Connections					
#	System Name, Acronym, and ITAB number	Owning Bureau and primary POC	Type of connection	Type of data and how it is shared	C&A Status of connected system
1.	Consular Lookout And Support System (CLASS) ITAB#: 558	Consular Affairs	Bi-directional	Applicant name check: i.e. no aliases present and verification of supplied information, via TCM. 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, 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.	ATO Expires: May 31, 2012
2.	Non-Immigrant Visa System (NIV) ITAB# 65	Consular Affairs	Bi-directional	Transfer of cases	ATO Expires: August 31, 2010
3.	Independent Namecheck (INK) ITAB#: 29	Consular Affairs	Bi-directional	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	ATO Expires: August 31, 2010

Shared System Connections					
#	System Name, Acronym, and ITAB number	Owning Bureau and primary POC	Type of connection	Type of data and how it is shared	C&A Status of connected system
				query function replaces the independent namecheck query function that was part of the IVO system.	
4.	Immigrant Visa Information System (IVIS) ITAB#: 49	Consular Affairs	Bi-directional	Transfer of cases	ATO Expires: August 31, 2010
5.	Diversity Immigrant Visa Information System (DVIS) ITAB#: 17	Consular Affairs	Bi-directional	Transfer of cases	ATO Expires: November 31, 2011
6.	Immigrant Visa Allocation Management System (IVAMS) ITAB#: 97	Consular Affairs	Bi-directional	Visa allocation management	ATO Expires: August 31, 2010
7.	Accountable Items (AI) ITAB#: 4397	Consular Affairs	Bi-directional	The Accountable Items module tracks and controls the valuable visa foils and passport forms.	ATO Expires: August 31, 2010
8.	Ten Print Live Scan System (TPLS) ITAB#: 829	Consular Affairs	Bi-directional	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.	ATO Expires: August 31, 2010

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. Information System Security Officers (ISSOs) determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance.

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 NIDS rules sets 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 to monitor computer usage and access to files are monitored. 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.

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. IVO 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. Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure appropriate data transfers, and storage methods are applied.

To reduce the privacy risks, access to information is controlled by application access controls. Every server on the CA OpenNet has NetIQ Security Manager installed, and it is used to monitor server activity. 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.

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 CCD datasharing arrangements for the following purposes:

- Checking the applicant's fingerprint information against DHS databases
- Establishing a record within DHS's Automated Biometric Identification (IDENT) system
- 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 will not go into the technical details on how the shared data is protected. See CCD System Security Plan (SSP) or CCD PIA for the security controls in place.

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 Consular Consolidated Database (CCD). When the CCD receives fingerprint requests or visa issuance data, the CCD forwards the information to the Department's datashare applications.

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 and interagency security agreement. 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.

The risk to privacy of sharing information contained in CTF with third parties is that the information provided will be used for unauthorized purposes, lost, stolen or misappropriated.

IVO information is shared with U.S. government agencies with a statutory requirement and 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 adhered to in order to ensure that any risk is addressed through the user-authorization process.

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* 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?

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:

- Form 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 (DHS) forms.

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

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

Information is given voluntarily by the applicants and with their consent, 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 Immigration and Nationality Act (INA). The information provided on the form and in the SORN regarding visa records 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?

The information in IVO is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application to the 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 or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the System of Records Notice (SORN), and in rules published at 22 CFR 171.31 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 171.32.

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 Privacy Act-covered, 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?

Internal access to IVO 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, authorized users must be an authorized user of the Department of State' unclassified network. Access to IVO requires a unique user account assigned by a supervisor. 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. 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.

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. ISSOs 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 security training and regular refreshment training.

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

All users must pass cyber security awareness training and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain 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.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly made inactive. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform--or may attempt to perform.

11. Technologies

a. What technologies are used in the system that involves 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 issue(s).

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, 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?

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 safeguarded and protected. Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. Department of State performs 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 for the triennial recertification of this system, IVO was certified and accredited for 36 months to expire on August 31, 2010.