

PIVOT PIA

1. Contact Information

A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services
--

2. System Information

(a) **Name of System:** Pre Immigrant Visa Overseas Technology

(b) **Bureau:** Consular Affairs

(c) **System Acronym:** PIVOT

(d) **iMatrix Asset ID Number:** 6654

(e) **Reason for Performing PIA:**

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

(f) **Explanation of modification (if applicable):**

3. General Information

(a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**

- Yes
- No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

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

PIVOT received an Authorization To Operate in December 5, 2012 for a period of 3 years.

The triennial Assessment and Authorization process is underway and PIVOT is expected to receive an Authorization-To-Operate by August 31, 2016.

(c) Describe the purpose of the system:

The Pre Immigrant Visa Overseas Technology (PIVOT) information system supports immigrant visa (IV) pre-processing at the National Visa Center (NVC), which includes immigrant visa case creation, immigrant visa package review, and support and inquiry functions. PIVOT interfaces with Consular Electronic Application Center (CEAC), electronic Document Processing (eDP), and Enterprise Appointment Management System (EAMS) to achieve paperless 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 Procedural Language / Structured Query Language (PL/SQL) application available on the Department's intranet (OpenNet) through the Consular Consolidated Database (CCD) Website. All PIVOT interfaces are brokered through CCD and Consular Affairs Enterprise Service Bus (CAESB) services, including the following examples:

- Petition data received from U.S. Citizenship and Immigration Services (USCIS);
- Case data and messages sent to and collected from CEAC;
- IV Interview appointment scheduling information received from EAMS in response to PIVOT requests.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

PIVOT collects and maintains PII for identification of foreign nationals applying for immigrant visas as well as U.S. Citizens or Legal Permanent Resident (LPR) petitioners and their legal representatives/agents. The sources of the information are systems which collect USCIS immigration petition data via the Computer Linked Application Information Management System 3 (CLAIMS3) and the Department of State immigrant visa application forms in CEAC.

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

- Names of Individuals
- Birthdates of Individuals
- SSN
- Phone number(s) of Individuals
- Personal Address
- e-mail address(es) of individuals
- Images of documents that may contain photographs and/or biometric IDs of applicants
- Individual financial information about applicants and case sponsors, including:
 - Annual income history

- Asset information
- Images of financial documents
 - W-2 Forms
 - 1099 Forms
 - Tax Returns and other tax documents
 - Affidavit of Support Forms
 - Proof of Asset Forms
 - Bank Statements
 - Social Security Administration Earnings Statements
- Images of police certificates from foreign countries
- Names and birthdates of applicant's spouse(s) and marriage place and date information
- Names and birthdates of applicant's children
- Names of applicant's parents
- Dates of applicant's previous travel to the U.S.
- Applicant education information
 - Name and location of school attended
 - Field of study
 - Type of degree and date obtained
- Applicant employment information
 - Employer name
 - Job title and description
 - Hours worked per week
 - Salary information
- Employment start and end dates
-

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1151-1363a (Title II of the Immigration and Nationality Act of 1952, as amended);
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 26 U.S.C. 6039E (Information Concerning Residence Status)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

SORN Name and Number: State-39 Visa Records

SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): October 25, 2012

No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

Yes

No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Yes

No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

Schedule number (e.g., (XX-587-XX-XXX)):

Length of time the information is retained in the system:

Type of information retained in the system:

A-14-001-02a Visa Case Files on Individual Aliens

Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: a. Case files on individual aliens issued an immigrant visa.

Disposition: Destroy 6 months after issuance.

DispAuthNo: N1-059-86-2, item 1a

B-09-002-01a Immigrant Visas

Issuances [Consular Consolidated Database]

Description: Information obtained from issued immigrant visa application forms (DS-230, 260, and related forms) and supporting documentation. Immigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographic data; adjudication data; visa class information; visa clearance and name check data; case summary data; case status data; and notes.

Disposition: TEMPORARY. Cut off at end of calendar year when issued. Destroy 11 years after issuance.

DispAuthNo: N1-084-09-02, item 1a

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. Cut off 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

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes
- No

If yes, under what authorization?

[26 U.S.C. 6039E](#) – Information Concerning Resident Status

(c) 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-600A, 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 National Visa Center (NVC).

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 petition data.

Updates to PII are submitted to the NVC electronically and via paper forms. The petitioner, applicant or legal representative can complete the paper immigrant visa form DS-230 or the electronic DS-260 available in CEAC. Information may also be collected through telephone and email exchange. Public inquiry response agents will then update the applicant's records within PIVOT.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

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 visually validate the authenticity and the completeness of the information received on the applicant from CEAC, DS-230, and DS-260, 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.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The case data initially captured in the PIVOT system is derived from the petition form submitted to the USCIS by the U.S. Citizens or Legal Permanent Residents (LPR) petitioner. As the case progresses and becomes eligible for processing by the Department of State, the PIVOT application interfaces with the Consular Electronic Application Center (CEAC) public-facing site to collect updated information on both the petitioner and applicant(s). Through CEAC, the individuals enter data and upload documentation that is transferred, through an established interface via the Consular Consolidated Database (CCD), to the PIVOT system. All updated information is applied to the PIVOT system.

In addition, the National Visa Center (NVC) provides a call center that the individuals may contact to inquire about the data captured and provide updates or corrections as needed.

(g) Does the system use information from commercial sources? Is the information publicly available?

United States Citizenship and Immigration Services (USCIS) petition data is retrieved from the CLAIMS3 system that 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 immigrant visa (IV) Package (Fees, Forms, and Documents). No other commercial information, publicly available information or information from other federal agency databases is used.

(h) Is notice provided to the individual prior to the collection of his or her 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/A, I-929) 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/forms> , for more details on the USCIS forms.

Department of State data collection is performed through CEAC. The web data-collection tool provides 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.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

- Yes
 No

If yes, how do individuals grant consent?

Yes, both immigrant visa petitioners and visa applicants have the right to decline to provide PII for use in processing immigration visa applications. However, failure to provide the information necessary to process the application may result in the petition being rejected or the immigrant visa application being denied. 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. 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.

If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PIVOT system is vulnerable to insider threat, unauthorized access, disclosure, modification and or misuse of the data by PIVOT users. In addition, there is the possibility, however unlikely, of an OpenNet security breach. These risks present privacy concerns for any PII collected. As a result, the PIVOT system was designed to minimize impact by limiting the collection of PII to the minimum required to perform the business function required of PIVOT.

5. Use of information

(a) What is/are the intended use(s) for 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 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) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the use of the information by PIVOT is relevant to the purpose for which the system was designed.

(c) Does the system analyze the information stored in it?

Yes

No

If yes:

(1) What types of methods are used to analyze the information?

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.

(2) Does the analysis result in new information?

New information is produced by PIVOT users and the comments are stored in PIVOT and relayed to the applicant, petitioner, or attorney through CEAC or written correspondence. Applicants resubmit corrected documents or submit missing documents to the NVC so that PIVOT users may complete the review of the applicant's case. PIVOT users can also add case comments that will be viewed later in IVO by IV processors and adjudicators overseas.

(3) Will the new information be placed in the individual's record?

Yes

No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

Yes

No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

PIVOT shares information internally with numerous State Department information systems listed below.

System Name and Acronym	Manner of sharing
Consular Consolidated Database (CCD)	Two-way
CA/CST Consular Affairs Enterprise Service Bus (CAESB)	Two-way
Immigrant Visa Allocation and Management System (IVAMS)	Two-way
Immigrant Visa Information System (IVIS)	Two-way
Enterprise Appointment Management System (EAMS)	Two-way

System Name and Acronym	Manner of sharing
Consular Electronic Application Center (CEAC)	Two-way
Immigrant Visa Overseas (IVO)	One-way: From PIVOT to IVO

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) What information will be shared?

System Name and Acronym	Type of data and how it is shared
Consular Consolidated Database (CCD)	The data from PIVOT is replicated to the CCD. This includes all core data and any requests or responses to other systems that are processed through the CCD. Responses and requests received on the CCD from other systems are returned to PIVOT from the CCD outgoing replication server.
CA/CST Consular Affairs Enterprise Service Bus (CAESB)	The Petition Data Query (PDQ) ESB service monitors the PIVOT request log for new requests for USCIS data. The PDQ service first searches Adoption Case Management Service (ACMS) data store of petition data previously received on a data feed from Department of Homeland Security (DHS). If no ACMS data match is found, PDQ then sends a web service call to USCIS PCQS for any related electronic petition data stored by DHS.
Immigrant Visa Allocation and Management System (IVAMS)	PIVOT executes a procedure to export the demand data that is delivered to IVAMS via email and mark the PIVOT records as reported. Qualifying and cutoff dates used by PIVOT are updated on the NVC database automatically via replication back from IVAMS through the CCD in the same manner as the data flows from IVAMS to the Posts.

System Name and Acronym	Type of data and how it is shared
Immigrant Visa Information System (IVIS)	<p>Two types of data are shared between IVIS and PIVOT.</p> <p>Case data from non-current IVIS cases that are about to become current is migrated from IVIS to PIVOT via shared database tables to aid in the creation of corresponding new IV cases in PIVOT (sharing of this data is one-way only, from IVIS to PIVOT). Once a case has been migrated from IVIS to PIVOT, all further processing of the case will take place in PIVOT only.</p> <p>Limited information about current IVIS cases that are ready to be scheduled for interview appointments is sent to PIVOT and forwarded to EAMS (see below); EAMS returns appointment dates and times to PIVOT for those cases, and PIVOT passes the information back to IVIS via shared database tables.</p>
Enterprise Appointment Management System (EAMS)	<p>PIVOT submits requests for new appointments, rescheduling, or cancellations (for both PIVOT and IVIS cases) to EAMS via a web service call. EAMS executes the requests based on case attributes (e.g., visa class) submitted by PIVOT and pre-defined post processing preferences then returns a response to PIVOT by a web service call.</p>
Consular Electronic Application Center (CEAC)	<p>Backend processes on the CCD monitor incoming replicated data from PIVOT for requests, responses, and messages that are needed by CEAC and Case Tracking (CTRAC). Routines are executed on the CCD to create CEAC messages on the CCD and push the data out to the CEAC DMZ database using Oracle Replication.</p> <p>The PIVOT system updates CTRAC tables on the local database that are replicated using Oracle Replication first to the CCD and then on to the CEAC DMZ database.</p> <p>The CCD monitors the CEAC package request log for entries targeted for PIVOT then executes routines to pull data/documents across the database link, format XML responses, and create return packages that are replicated out from the CCD to PIVOT.</p>
Immigrant Visa Overseas (IVO)	<p>Backend processes on the CCD monitor incoming replicated data from PIVOT for cases in Transfer Ready status then executes the procedures to populate IVO shadow tables that are pushed out to the target post via Oracle Replication.</p>

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.

(c) What is the purpose for sharing the information?

The data is shared among the numerous systems in an effort to help them complete their business functions whether that is internally with the State Department information interconnected systems or externally between the State Department and DHS USCIS. Ultimately, the data is shared with the consulates to facilitate the adjudication of visas by consular officers.

(d) The information to be shared is transmitted or disclosed by what methods?

The information is shared by direct connections with other consular systems (CCD, CAESB, IVAMS, IVIS, EAMS, and CEAC), and email. All of these activities and systems reside on the Department's secure OpenNet network.

Information shared externally (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.

(e) What safeguards are in place for each internal or external sharing arrangement?

PIVOT mitigates 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 Interconnection Service Agreement, which outlines controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

**(f) What privacy concerns were identified regarding the sharing of the information?
How were these concerns addressed?**

Privacy concerns associated with PIVOT processing of PII include insider threat, unauthorized access, disclosure, modification and or misuse of the data by PIVOT users. 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.

Vulnerabilities and risks are mitigated through the system's certification process. National Institute for Science and Technology (NIST) recommendations are strictly

implemented 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. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The U.S. Citizen or Legal Permanent Resident (LPR) petitioners and sponsors associated with cases captured by PIVOT may gain access to their information via communication with the National Visa Center (NVC). The NVC provides a call center that the individuals may contact to inquire about the data captured and provide updates or corrections as needed. In addition, these individuals can also communicate with the NVC through the Consular Electronic Application Center (CEAC) public facing site. All information captured by CEAC, is transferred through an established interface via the Consular Consolidated Database (CCD) to the PIVOT system. Individuals may view and update contact email addresses using CEAC. Individuals may also submit updated paperwork with other personal data by uploading documents to CEAC that are also transferred to PIVOT where the data is ingested and updates or corrections can be made. Once the petitioner or sponsor has uploaded documents, they are not viewable or downloadable, even by the same user.

The applicant and intending immigrant may gain access to their information in the same manner as the petitioner and sponsor. However, they are also required to submit an online application to the Department of Status using CEAC. At any time from when they begin filling out this application, the applicant has access to review the data entered.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes

No

If yes, explain the procedures.

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 by telephone or email. Processing Specialists at the NVC will update case data at the request of the IV applicant. Processing Specialists at the NVC 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.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Visa applicants will be contacted via email if there is a need for previously submitted information to be corrected. The applicants would be directed to log into a specific public facing website to update their data online. Procedures for notification and redress are published in the SORN State-39 and in rules published at 22 CFR 171 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.

8. Security Controls

(a) How is the information in the system secured?

Various management, operational, and technical controls are in place and are tested as least annually to verify data stored, processed, and / or transmitted within PIVOT is at a low risk of compromise.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

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 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. Authorized users authenticate to OpenNet using their user computer access card (CAC) and pin. Once logged on to OpenNet, PIVOT users access their local CCD Portal and then click the Logon button on the home page, which then prompts them for their PIVOT credentials to enable them to gain access to the PIVOT menu.

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 recapitulates the restrictions on the use of the system.

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 and privacy training is required for all authorized users.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Numerous management, operational, and technical safeguards are in place to protect data within the PIVOT information system. In order to have access as a PIVOT user an individual must be a State Department employee or contractor, have a network account, receive access to data specific to their assigned job role, utilize both password and common access card controls and pass through various layers of physical security. In addition, auditing of numerous activities performed on the information system are logged for possible future investigations. 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. Therefore, 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.

(d) Explain the privacy training provided to authorized users of the system.

All users must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the information system. In order to retain the access, users must complete annual refresher training. Additionally, all persons that work with PII must take PA-459, a course entitled Protecting Personally Identifiable Information or a comparable course.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

Yes

No

If yes, please explain.

The PIVOT security and privacy controls in place are adequate to safeguard customer privacy. PIVOT utilizes numerous management, operational and technical security controls to protect the data in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). 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), and audit reports.

(f) How were the security measures above influenced by the type of information collected?

Due to the nature and volume of data collected by the system, several measures were taken in the design of PIVOT to reduce risk to data security and integrity. Specifically, more granular access controls and auditing were implemented.

The access and actions of individual PIVOT users is controlled at a very granular level. Users are granted access as trainees or fully trained staff to each system function based on their need to access those function and training level for those specific functions. In addition, many of those grants are further refined based on the type of case being handled by those functions.

All access and actions of PIVOT users is audited. Each function and case accessed by a user is recorded. Each change to user authorization is recorded. To provide additional insurance with respect to preserving data integrity, an additional audit layer was added which records every change to data in the system. A snapshot is taken with each data change so that the previous state is saved along with who made the change and when it was made.

9. Data Access

(a) Who has access to data in the system?

Bureau of Consular Affairs post officers/users, system administrators, and database administrators have access to data in the information system.

(b) How is access to data in the system determined?

Access to data in the system is determined by an individual's job role, hence need to know. Job roles are set up with least privilege in mind to allow for a task to be completed with only the requisite access necessary. Access control lists define who can access the system and at what privilege level, accounts are regularly reviewed, and inactive accounts are promptly deleted.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

Yes

No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Information access will be restricted to authorized users based on the specific job roles of each user. This is referred to as "need to know" and "least privilege". The user will only have enough access to perform their job and nothing more.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

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.