PRIVACY IMPACT ASSESSMENT

Pre-Immigrant Visa Overseas Technology (PIVOT)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Pre-Immigrant Visa Overseas Technology (PIVOT)
(b) Bureau: Consular Affairs (CA)
(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 is currently undergoing its Assessment and Authorization to receive its Authorization to Operate (ATO). The estimated ATO date is Spring 2021.

(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, support and inquiry functions. The PIVOT application is used by consular officers to adjudicate immigrant visa (IV) cases overseas and provides domestic centers the capability to support paperless IV application processes. The CA Consular System and Technology (CST) office designed PIVOT to handle Department of State processing of IV cases from receipt of the paper petition shipped from United States Citizenship and Immigration Services (USCIS) to the point when the case is ready for transfer to an overseas post. PIVOT's core functions support the NVC staff in case creation, document review, and inquiry support.

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

PIVOT collects the following information on non-U.S. citizens/non-LPRs:

- Name
- Birthdate
- Birthplace
- Social Security Number
- Personal Phone number
- Personal address
- Personal email address
- Nationality
- ____Education information
- Employment information
- ___Family Information: Names and birthdates of applicant’s spouse and children
- ___Names of applicant’s parents
- Legal Information
- ____Business contact information: name, work address, work phone number and legal representation business information

PIVOT collects the following PII on U.S. Citizens:

- Name
- Business contact information: work address, work phone number, and legal representation business information.

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

- 8 U.S.C. §§ 1101-1363a (Titles I and 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)
- 26 U.S.C § 6039E – Information Concerning Resident Status
- International Narcotics Control – Title IV of the Anti-Drug Abuse Act of 1988, PL 100–690, November 18, 1988
- 8 C.F.R § 245.1(a)
- 22 C.F.R. Parts 40-42, and 46 (Visas)

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

☒Yes, provide:

- SORN Name and Number: Visa Records – STATE-39; June 15, 2018

☐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 Office 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:

Schedule number: B-09-002-08a and 8b
Length of time the information is retained in the system: Temporary. Cutoff at the end of the calendar year when issued. Destroy 5 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: IVO maintains immigrant visa issuance and refusal case record data on local area network databases.

Schedule number: B-09-0020-10
Length of time the information is retained in the system: Temporary. Destroy 5 years after the project/activity transaction is completed or superseded, or the associated system is terminated, or the associated data are migrated to a successor system.
Type of information retained in the system: CCD, IVO and NIV System Documentation. System specifications, file specifications, user guides, data dictionaries, and related technical documentation.

Schedule number: B-09-002-17
Length of time the information is retained in the system: Destroy when 1 year old unless document pertains to an individual alien resident of the consular district who may be mandatorily ineligible for a visa, in which case retained indefinitely.
Type of information retained in the system: Information copies of communications from other posts that are not required for incorporation in the visa general subject file.

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>are</u> US citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are <u>not</u> U.S. Citizens or aliens lawfully admitted for permanent residence)

(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?

PIVOT does not collect any PII from individuals directly. All PII processed by PIVOT is sourced from other systems and manual processes including the following:

- Paper petition cases mailed by the applicant, petitioner, or the legal representative are shipped from the United States Citizenship and Immigration Services (USCIS) to the Department of State National Visa Center (NVC) and scanned into the Consular Affairs, Visa Information System (IVIS). PIVOT receives information on the petition cases from IVIS electronically. The following USCIS forms currently apply:
  I-797 Notice of Action
  I-864 Affidavit of Support under Section 213A of the INA
  I-864A Contract between Sponsor and Household Member
  I-864EZ Affidavit of Support under Section 213A of the INA
  I-864W Request for Exemption for Intending Immigrant's Affidavit of Support
  I-130 Petition for Alien Relative
  I-800 Petition to Classify Convention Adoptee as an Immediate Relative
  I-526 Immigrant Petition by Alien Entrepreneur
  I-129F Petition for Alien Fiance/Spouse
  I-600 Petition to Classify Orphan as an Immediate Relative
  I-730 Refugee/AsyleeRelative Petition

I-360 Petition for Amerasian, Widow(er), or Special Immigrant
I-929 Petition for Qualifying Family Member of a U-1 Nonimmigrant
I-140 Immigrant Petition for Alien Worker
I-600A Application for Advance Processing of an Orphan Petition
I-824 Application for Action on an Approved Application or Petition

- Applications for the Immigrant Visa and Alien Registration Form, (DS-230), or the electronic Immigrant Visa and Alien Registration Application, (DS-260), available in the Consular Electronic Application Center (CEAC) system is transferred electronically to PIVOT via the Consular Consolidated Database (CCD).

- Updates to petitioner information may also be collected through telephone and email exchange from DHS/USCIS and CA Visa Offices. Department of State Public Inquiry Response Agents will then update the applicant's records within PIVOT.

(c) 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.

(d) 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 representative filing on behalf of the applicant with the respective source system. Also, Department personnel at NVC visually validate the authenticity and the completeness of the information received on the applicant from CEAC, form DS-230, and form DS-260 before transferring the case to the post. CEAC interfaces with CCD which provides information flow to PIVOT. Additionally, certain fields are validated for accuracy through comparison of available documents submitted as part of the application process for the specific service being requested (e.g., dates of birth entered are compared to the dates on birth certificates when submitting a DHS I-130 application).

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

Yes, as the case progresses and becomes eligible for processing by the Department of State, the PIVOT application information is updated. Through CEAC, applicants enter updated information 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. (CEAC and CCD are not within the boundary of this 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.

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

No, PIVOT does not use commercial or publicly available information.

(e) Is notice provided to the individual prior to the collection of his or her information?

PIVOT does not collect information directly from individuals. Information in PIVOT is received from the DHS/USCIS and other CA systems (CEAC, CCD). The source systems where the applicant's information is entered and USCIS provide the required notice to applicants. (This process is not within the boundary of this PIA).

(f) 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?

If no, why are individuals not allowed to provide consent?
PIVOT cannot be not accessed by the public. Applicants would consent via the source systems/agency (USCIS) where applications are submitted. The source systems would provide the notice and consent at the collection point.

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

The PII collected by PIVOT is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the functions for which it is intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the PII in PIVOT is to validate and assess information provided by applicants to support decision making of the PIVOT Consular staff in the review of IV petition applications.

(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 PII in PIVOT is required to support the visa application submission, processing, and approval/denial decisions.

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

☐Yes

☒No. PIVOT does not analyze information.

If yes:

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

(2) Does the analysis result in new information?

(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.

The term “internal sharing” traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as “bureau” at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in the PIVOT system will be shared internally database to database with the CA system Consular Consolidated Database (CCD). CCD interfaces with the following systems that are a part of the PIVOT information flow, but not directly connected: Consular Affairs Enterprise Service Bus (CAESB) - monitors request logs in CCD that initiates a request for USCIS data; Immigrant Visa Allocation Management System (IVAMS), Consular Electronic Application Center (CEAC).

The following Consular Affairs sytems are electronically connected database to database with PIVOT: Electronic Document Processing (eDP), Immigrant Visa Information System (IVIS), and Enterprise Appointment Management System (EAMS).

There is no sharing of information with external systems with PIVOT.

(b) What information will be shared?

The personally identifiable information (PII) listed in paragraph 3d is shared internally with the CA systems listed in 6a above.

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

The data are shared with posts via aforementioned CA systems to facilitate the adjudication of visas by consular officers.

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

PIVOT information shared among Consular Affairs systems is via database to database. The information is shared by secured internal connections with other consular systems (CCD, EAMS, IVIS, eDP) and email. All of these activities and systems reside on the Department's secure intranet network, OpenNet. All physical records printed for processing purposes are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only.

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

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Safeguards in place for internal sharing arrangements include secure transmission methods (Hypertext Transfer Protocol (HTTP) via Secure Sockets Layer (SSL) with multiple Transmission Control Protocol (TCP) layers). The security program involves the establishment of strict rules of behavior required by security controls for each major application, including PIVOT. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. Additionally, regularly administered security and privacy training informs authorized users of proper handling procedures.

There is no sharing of information with external systems with PIVOT.

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

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:
   Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure of information to unauthorized parties and/or theft of information regardless whether the motivation is monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

2) Strict role based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level.

3) System authorization and accreditation process along with continuous monitoring via Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

4) All communications are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

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

Users can review the PII text data associated with their visa applications via the Consular Electronic Application Center (CEAC) system, which is external to PIVOT, but they cannot view the electronic documents that NVC attached to the case. U.S. citizen, LPR petitioners, and sponsors with cases captured by PIVOT may also gain access to their information via communication with the National Visa Center (NVC). The NVC provides a call center that individuals may contact to inquire about their case or to make updates and corrections. Applicants may also communicate with the NVC through the Consular Electronic Application Center (CEAC) public-facing site.

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

☒Yes ☐No

If yes, explain the procedures.

Consular officers who adjudicate Immigrant Visa cases maintain contact with applicants during the process and can assist in addressing inaccurate or erroneous information. The IV applicant may also submit updates to contact information in the form of email addressed through the CEAC public-facing site. Until the full IV package and application are submitted, the IV applicant may submit updated information through the 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 the CEAC requesting updated or corrected information. These corrections are made directly in the 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:

1. Correspondence previously sent to or given to the applicant by 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?

Individuals are notified of the procedures to correct records in this system by a variety of methods:

1. During their visa interview and visa processing
2. Published SORNs
3. Instructions on forms and web pages (or links to Agency Privacy Policy)
4. Being notified by letter that a correction is needed

Each method contains information on how to amend records and contact information.

8. Security Controls

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

The information in PIVOT is secured within the Department of State intranet where risk factors are mitigated through the use of defense in-depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Department of State user access to PIVOT is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user’s supervisor and the local Information System Security Officer (ISSO).

PIVOT is configured according the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the

Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 security and privacy controls, that consist of privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(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.

To access the PIVOT system, persons must be authorized users of the Department of State's unclassified internal network (OpenNet), which requires a background investigation and an application approved by the supervisor and local Information System Security Officer (ISSO). Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to PIVOT is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Local Information System 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.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with State Department Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the PIVOT audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

If an issue were to arise, administrators of the system would review (audit) the logs collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training which has a privacy component to access or use the systems. Additionally, Department of State personnel are required to take the biennial course PA318 (Protecting Personally Identifiable Information). The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit are encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

The consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, damage to standing or reputation, financial loss to the Department of State or individuals, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

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 is determined based on role-based user requests which are approved by the supervisor and local ISSOs. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Yes, procedures and controls are documented in the PIVOT System Security Plan.

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

Only System Administrators have access to all data in the system. Separation of duties and least privilege are employed and users have access to only the data that the supervisor and the local ISSO approves to perform official duties. Users of PIVOT consist of Department of State personnel and contractor personnel.

PIVOT Users
User access controls determine how, when, and where PIVOT users will gain access to the system. These users can view all the data, but there are restrictions as to what data each user is allowed to access. PIVOT users are assigned to various roles that allow them to perform duties commensurate with their job function. The following are examples of the PIVOT user group roles within PIVOT: data entry, case view, problem resolution, pre-entry duplicate user, operations personnel, and security manager.

Once a user is properly identified and authenticated by the system, the user is authorized to perform all functions commensurate with user’s job requirements.

System Administrators
System administrators are authorized to access PIVOT for the purpose of performing maintenance, troubleshooting technical issues, installing software and patches, and other actions needed to keep PIVOT operational. They have access to all the data and are responsible for all

daily maintenance, backups, establishing access control lists (ACLs), and maintaining user accounts. They have logon identifications associated with their name for the purpose of auditing.

Database Administrators

Database Administrators have access to PIVOT information based on specific roles. They are responsible for all daily maintenance, backups, and maintaining backend database user accounts. The access of PIVOT database administrators is limited to only those application files necessary to perform the ~~speficic~~specific authorized daily activities. This limit of access is controlled through the use of access control lists (ACLs) as established by the system administrators.

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

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks and is implemented. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN), and activities while logged in can be traced to the person who performed the activity.