Federal Bureau of Investigation

Privacy Impact Assessment
for the
[Passport Visa Database (PVDB)]

<u>Issued by:</u>
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: December 11, 2020

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Passport/Visa database (PVDB) is an application that assists FBI employees, contractors, and detailees (FBI personnel) obtain official and diplomatic passports and visas, and serves as a central repository for all current and historical information concerning official international travel by FBI personnel. FBI personnel are sometimes required to travel internationally on official business or deploy overseas with the Legal Attaché Program in order to assist FBI operations from around the globe. Passports, and occasionally visas, are required for these activities. Therefore, efficient and swift access to travel documentation information is crucial to carrying out the FBI's mission. The Passport and Visa Program Office, Logistics and Official Travel Unit (LOTU) utilizes PVDB to obtain all official and diplomatic passports and visas that are issued to FBI employees, their qualifying family members, and Task Force Officers (TFOs).[1] PVDB also enables LOTU personnel to create various reports on passports and visas for the Department of Justice (DOJ), FBI executives, FBI Headquarters (FBIHQ) divisions, and Field Offices (FOs).

PVDB is a web-based application that resides on the FBI's Oracle Exadata Database Machine server and is accessed via the FBI's Secret Enclave (FBINet).[2] System users manage, edit, and display data within the Oracle Database.

Section 208 of the E-Government Act of 2002, P.L. 107-347 requires that agencies conduct PIAs on information technology systems that collect and maintain identifiable information regarding individuals, and, if practicable, to make such PIAs publicly available. Accordingly, this PIA has been conducted and will be made publicly available. As changes are made to PVDB, this PIA will be appropriately reviewed and revised.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

Purpose

[1] In some instances, LOTU (and PVDB) may keep track of travel documentation for the Attorney General or other Department of Justice personnel who travel on official FBI business.
[2] FBINet is a secure FBI network that is accredited to handle and store information classified at the Secret level. It is covered by separate privacy documentation.

PVDB allows LOTU personnel to monitor the status of official passports and visas ("official travel documents") issued to FBI employees, their qualifying family members, and TFOs. Using PVDB, LOTU personnel track passport and visa applications as well as correspondence with the Department of State (DoS) and applicants (the content of the applications and correspondence is not captured). Specifically, the system supports the passport/visa management process as follows:

- <u>Passports</u>: When a passport is needed for official FBI business, the requesting individual accesses the DoS website from any unclassified network and completes a passport application form online.[3] The employee prints a hard copy of the form(s) and provides a signed copy of the form, along with proof of citizenship (e.g., birth certificate, old passport) and a passport photo, to the FBI's Passport and Visa Program Office. LOTU personnel then create a new record in PVDB for the individual submitting the passport application packet. All personal information about that individual is automatically populated in PVDB from the Human Resources Source System (HR Source).[4] Once a PVDB record has been created, the system automatically generates a letter of authorization, which LOTU personnel hand carry to DoS, along with the official passport application packet. DoS then determines whether to issue the requested passport(s). Once issued, LOTU personnel retrieve the passport at DoS and then manually add the passport information to PVDB.

- <u>Visas</u>: If a visa is needed for FBI official travel, the requestor completes the pertinent DoS visa application form and submits the application, along with the official or diplomatic passport and visa photographs to the FBI's Passport and Visa Program Office. LOTU personnel hand carry visa applications to the relevant embassy or consulate for approval and issuance. Once issued, LOTU personnel retrieve the visa and then manually add the applicable visa information to the requestor's existing PVDB record.

For passports and visas of qualifying family members, the requestor is responsible for ensuring that any appropriate applications are completed, and required documentation is provided to the Passport and Visa Office.

PVDB also has the ability to create internal reports about official passports and visas. Reports are broken into two categories: standard reports and interactive reports. System users can access the reports by navigating to the "reports" or "interactive reports" tabs within PVDB.

- <u>Standard reports</u>: Standard reports are generally used to provide situational awareness to FBI executives, FOs, and other FBI entities. Examples of standard reports include:
    - A listing of all issued passports and/or all issued visas;
    - A listing of all cancelled visas;
    - A listing of pending passports at DoS; and
    - A listing of pending visas.

[3] The online passport application system is owned by DoS and not the FBI. The DoS is responsible for privacy documentation for the passport application system.
[4] HR Source is the FBI's internal Human Resources system. It is covered by separate privacy documentation.

- Interactive reports: Interactive reports, on the other hand, are custom-created via a dropdown menu, and can include any category of information captured in PVDB.

LOTU personnel can generate standard reports as a PDF file, or interactive reports as a text file, Excel spreadsheet, or PDF. Once generated, reports are disseminated to appropriate parties via hard copy or FBINet email.

Additionally, PVDB writes audit logs to a separate back-end application: Central Activity Tracking for Oracle Application Express (CATFOX).[5] PVDB uses CATFOX to record system activity and provide an audit capability to ensure that individuals use the system properly. The audit logs record all data activity, including: who logs on (identified by FBINet username); date and time of logon; how many times a user logs on over the life of the system; inappropriate or unusual activity; inactivity, the date and time a user creates a record; and the date and time a user updates a record. Audit logs are reviewed as least weekly, and vulnerability/compliance scanning occurs monthly. CATFOX audit records cannot be altered or deleted. Only users with an Admin role have access to CATFOX.

Users

Approximately forty individuals have access to information in the system. Only personnel in LOTU have editing and modifying capabilities. PVDB utilizes role-based access to ensure information is only accessed by authorized personnel.[6] Any unauthorized person attempting to access PVDB receives an error message and is denied access. In addition, an invalid access attempt record is transmitted to CATFOX memorializing the FBINet username and the date/time of the invalid access attempt.

PVDB users are assigned one of four roles:

1. Admin: Admin users can view and add/edit/delete all categories of front-end and back-end information. Additionally, Admin users can add additional users, assign user roles, and generate reports.[7]

2. Owner: System Owners are able to view all categories of front-end information and add/edit/delete such information in the database. System Owners can add/edit/delete passport/visa information, add additional users, assign user roles, and generate reports. Currently the LOTU Unit Chief and Supervisory Management and Program Analyst have System Owner access.

3. General user (i.e. “Modify”): General user is the default user role for LOTU personnel. General users are able to view all categories of front-end information, and can generate reports from the system. While general users are able to add or edit passport/visa information, they cannot delete information.

[5] CATFOX is covered by separate privacy documentation.
[6] Role-based access assigns user roles based on official duties; the user has access only to the particular information authorized for that user role.
[7] Admin users also have access to audit logs via CATFOX.

4. Read-only: Approximately thirty individuals have read-only access to PVDB. These users have been granted access to PVDB for operational purposes. Read-only users include personnel from operational units that need to send FBI personnel abroad on short notice and need to know if specific FBI personnel have active passports or visas for certain countries.

Additionally, the Enterprise Process Automation System (EPAS)/Beacon,[8] the Asset Management System (AMS),[9] and the Enterprise Security Operations Center (ESOC)[10] have read-only access to PVDB information to support the specific functions of these systems, which are described in greater detail under System Interconnections, infra. These systems do not, however, have access to the PVDB database, but only to links or snapshots of certain PVDB information.

Users access PVDB by logging onto their FBINet workstation and opening a web browser such as Internet Explorer, Firefox, or Google Chrome. Users must then navigate to the PVDB website. A separate username or password is not required, as PVDB relies on single sign-on authentication utilizing the user's FBINet username and password. After login, users are presented with different options based on their user role:

- System Admin: System Admins are allowed five options: 1) Passports/Visa; 2) Reports; 3) Interactive Reports; 4) Owner Administration; and 5) Database Administration. **Passports/Visa** allows users to review and enter passport and visa information. **Reports** and **Interactive Reports** allow users to generate reports, as previously described. **Owner Administration** allows users to create, modify, or assign roles to other PVDB users. **Database Administration** allows users to update general information that affects the entire PVDB, such as countries, offices, and passport and visa categories. This information then pre-populates PVDB dropdown boxes.

- System Owner: System Owners are allowed four options: 1) Passports/Visa; 2) Reports; 3) Interactive Reports; and 4) Owner Administration. System Owners cannot perform **Database Administration** functions or assign users as System Admins.

- General User: General Users are allowed three options: 1) Passports/Visa; 2) Reports; and 3) Interactive Reports. General Users cannot perform **Owner Administration** or **Database Administration** functions.

- Read-only Users: Read-only users can access Passports/Visa information and run reports, but cannot add, edit or delete information.

Data Input, Output and Retrieval

[8] EPAS and Beacon are covered by separate privacy documentation.
[9] AMS is covered by separate privacy documentation.
[10] ESOC provides the FBI with the ability to conduct real-time monitoring and security analysis of FBI Information Technology systems. ESOC has three systems: EDOC 1, ESOC 2, and ESOC 3. ESOC 2 provides the monitoring environment for the FBINet (which is where the PVDB resides). The ESOCS are covered by a separate privacy documentation

Employee information (e.g., name, title, grade and service level) is automatically populated with information from HR Source. Qualifying family member information, as well as all passport and visa information, is manually entered by LOTU personnel.

Information is generally transmitted from PVDB in standard and interactive reports. PVDB also automatically writes audit logs to CATFOX for auditing purposes.

To retrieve information about an individual, users navigate to the Passports/Visa screen and enter the name of the FBI employee or TFO into the free form search bar. (Information about qualifying family members will be nested under these records.) Relevant search results will then be presented.

System Interconnections

PVDB interconnects with the following systems:

- HR Source: When LOTU personnel create a new record in PVDB by entering an individual's name into the database HR Source is the FBI's internal Human Resources system. HR Source automatically populates PVDB with personnel information (e.g., title, grade and service level, etc.).

- EPAS/Beacon: EPAS is an automated workflow tool that uses data from PVDB for the FBI's Beacon system. Beacon is the International Operations Division's automated process for coordinating official travel outside of the United States. Passport/visa data in PVDB is transmitted to EPAS (and subsequently to Beacon) via a one-way database link.

- ESOC's FBINet Monitoring Network: ESOC is responsible for the security of FBI networks, including protecting networks against potential malicious activity by members of the FBI workforce. ESOC has a one-way interface (and read-only access) with PVDB. Data transfers from PVBD to ESOC occur via direct connections between interface components.

- CATFOX: PVDB shares a direct link with CATFOX to write audit logs to CATFOX.

- AMS: PVDB interconnects with AMS, which maintains records regarding the use, maintenance, and disposition of property issued to FBI personnel, including official and diplomatic passports. FBI employees, their family members, and TFOs must return official travel documents to the FBI upon the employee's separation/retirement, or the termination of a TFO's assignment to an FBI task force. AMS receives passport/visa information from PVDB through a one-way database link.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	28 U.S.C. 33, Sec. 533
X	Executive Order	E.O. 12333, Sec. 1.3(b)(20)(A) E.O. 12333, Sec. 1.4(h)

		E.O. 12333 Sec. 1.5(g) E.O. 13388 E.O. 13356
X	Federal Regulation	28 C.F.R. 0.85(a) 28 C.F.R. 0.85(d) 28 C.F.R. 0.85(l)
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

Information in PVDB is organized and stored under the requesting FBI employee or TFO's name. There are three primary types of information held in PVDB: 1) information relating to the requesting individuals and their family members, if applicable; 2) passport information; and 3) visa information.

1. Information about individuals:

For FBI employees and TFOs, the information maintained in PVDB includes the individual's name, office, cost code, title, grade and service level, date of birth (DOB), employee status (active or inactive), employee type (i.e., agent, professional staff, TFO), and Social Security number (SSN). For family members, the information includes name, DOB and SSN, and the record is designated as belonging to a family member rather than an employee.

2. Passport information:

Passport information contained in PVDB includes: the name of the LOTU personnel creating a record; passport number; passport type; whether the application is expedited; dates of travel (if available); date the application was received by LOTU; date the application was delivered to DoS; date the passport was retrieved from DoS; passport issuance and expiration dates; and the date and reason the passport became inactive, if applicable. The system also contains a free form comments section for any additional information relevant to a passport application and issuance, e.g., whether a marriage certificate was included and returned or a photo was missing from the application packet.

3. <u>Visa information</u>:

Visa information maintained in PVDB includes: visa type (e.g., multiple, single, double, diplomatic, transit); the country of issue; the date the application was received by LOTU; the date the application was delivered to the pertinent country's embassy/consulate; the scheduled (and actual) visa pick-up dates; the travel dates covered by the visa; and the date the passport/visa was sent to the requestor. PVDB also includes the names of LOTU personnel who transport the visa documents to and from the foreign embassy/consulate. A free form comments section contains any additional information relevant to the visa application and issuance, e.g, the date the traveler requested visa status information.

(1) General Categories of Information that May Be Personally Identifiable	(2)
	Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)
		(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Name	X	A, B, C, D	Applicants include FBI employees, contractors and detailees (A, B); family members include members of the public (C, D)
Date of birth or age	X	A, B, C, D	same
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	same
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number	X	A, B, C, D	same
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- Photographs or photographic identifiers			
- Video containing biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			
Visa Country	X	A,B,C,D	
Visa Type (cancelled, diplomatic, double entry, multiple entry, one year, single entry, transit)	X	A,B,C,D	
Date arrived in passport visa office	X	A,B,C,D	
FBI employee/contractor/detailee who prepared the letter to go to DoS	X	A,B,C,D	
Dates passport delivered to/retrieved from Embassy/DoS	X	A,B,C,D	
Initials of the FBI employees/contractors/detailees who couriered the passport back and forth from the embassy,	X	A,B,C,D	
Date the visa was sent to the traveler	X	A,B,C,D	
Estimated date of travel	X	A,B,C,D	
Date the visa was issued	X	A,B,C,D	
Date the visa expires	X	A,B,C,D	
Run date	X		
Fedex tracking number	X	A,B,C,D	
Scheduled pick up date of the passport from the State Department	X	A,B,C,D	
Comments about the passport or visa application or about the actual passport or visa	X	A,B,C,D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

Actual date of travel	X	A,B,C,D	
UEID	X	A	
FBI Field Office	X	A	
FBI cost code	X	A	
Date the passport application was received by LOTU	X	A,B,C,D	
Passport type (primary, diplomatic secondary, diplomatic, personal, secondary, service, Taiwan)	X	A,B,C,D	
Pending visa application (Yes or No)	X	A,B,C,D	
Expedite application (Yes or No)	X	A,B,C,D	
Initials of the FBI employee/contractor/detailee who prepared the formal letter that accompanies the passport request	X	A,B,C,D	
Date application was taken to DoS	X	A,B,C,D	
Initial date of travel (from passport)	X	A,B,C,D	
Comments about the passport application or the passport itself	X	A,B,C,D	
FBI email address	X	A	
Employee status (A = active, I = inactive)	X	A	
Employee type (e.g., Relative, Agent, Contractor, Detailee)	X	A,B,C,D	
Date passport was sent to applicant from the FBI or the date the passport was given to the FBI employee	X	A,B,C,D	
Date the passport came back from DoS	X	A,B,C,D	
Date passport was issued	X	A,B,C,D	
Date passport expires	X	A,B,C,D	
Fedex tracking number for the passports that are sent to the field office where the FBI person works	X	A,B,C,D	
Date the passport became inactive	X	A,B,C,D	
Comments about the inactive passport	X	A,B,C,D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to:
		A. DOJ/Component Employees, Contractors, and Detailees;
		B. Other Federal Government Personnel;
		C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);
		D. Members of the Public - Non-USPERs
			(4) Comments

System admin/audit data - Activity Type (Delete, Insert, Invalid Access, Invalid Credentials, Successful Login, Update), -Data accessed	X	A	

3.2 *Indicate below the Department's source(s) of the information. (Check all that apply.)*

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone	X	Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): DoS					

Non-government sources:					
Members of the public	X*	Public media, Internet		Private sector	
Commercial data brokers					
*For passports and visas of qualifying family members, although the FBI employee or TFO is responsible for ensuring that any appropriate documentation is provided to the Passport and Visa Office, the family members themselves may provide the underlying information.					

Section 4: Information Sharing

4.1 *Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.*

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the Component		X		Information is shared within the component via system interconnections, as follows: HR Source: HR Source is the FBI's internal Human Resources system. HR Source automatically populates PVDB with basic personnel information (e.g., title, grade and servce level, etc.) when LOTU personnel create a new record in PVDB by entering an individual's name into the database. EPAS/Beacon: Beacon is the International Operations Division's automated process for coordinating official travel outside of the United States. Official passport/visa data about FBI personnel only needs to be entered into PVDB; the data is then transferred from PVDB into EPAS via a one-way database link, and is then transferred into Beacon from EPAS. (ESOC's FBINet Monitoring Network: ESOC is responsible for the security of FBI networks, including protecting networks against potential malicious activity by members of the FBI workforce. ESOC relies on multiple datasets, including PVDB, to help identify these types of threats. ESOC has a one-way interface (and read-only access) with PVDB. Data transfers from PVDB to ESOC occur via direct connections between

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
				interface components. CATFOX: PVDB also shares a direct link with CATFOX in order to write audit logs to CATFOX. AMS: AMS receives information from PVDB through a one-way database link. AMS maintains records regarding the use, maintenance, and disposition of property issued to FBI personnel, including official and diplomatic passports. FBI employees, their family members, and TFOs must return official travel documents to the FBI upon the employee's separation/retirement, or the termination of a TFO's assignment to an FBI task force.
DOJ Components	X			
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

It is not anticipated that PVDB data will be released to the public under the circumstances contemplated by this question.

<u>Section 5:</u> Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Notice is provided pursuant to the following system of records notice published in the Federal Register: *The FBI Central Records System*, JUSTICE/FBI-002, 63 Fed. Reg. 8671 (Feb. 20 1998), as amended; *DOJ Computer Systems Activity and Access Records*, DOJ-002, 64 Fed. Reg. 73785 (Dec. 30, 1999), as amended. These SORNs provide general notice regarding the entities with and situations in which the FBI may use and disseminate the records in this system. The published routine uses and blanket routine uses applicable to this system provide additional notice about the ways in which information maintained by the FBI may be shared with other entities.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals that do not participate in the collection, use or dissemination of information in the system will be ineligible for official travel or job opportunities requiring an official or diplomatic passport or visa. To the extent official travel is required for successful job performance, failure to participate may result in adverse employment actions.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

All PII in PVDB is provided by the individual whose official duties require a passport or visa. Such information, whether unique to PVDB or contained in another or multiple FBI systems, can be updated or accessed by the individual, at any time, via enterprise and system specific processes for the duration of the individuals FBI employment or assignment.

<u>Section 6</u>: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** PVDB resides on the Joint Enterprise Development Infrastructure Initiative (JEDII), which has an ATO that expires on 7/17/2020. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** JEDII currently supports approximately 18 systems, several of which provide direct support to FBI investigative activity. As such, the summary or release of POAMs would pose risks to the component. Information Systems Security Officers (ISSOs) are involved in monitoring the security of systems and routinely ensure security vulnerabilities are identified and corrective action is taken as necessary to meet FBI IT security standards.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** PVDB shares a direct link with CATFOX to write audit logs. The audit logs consist of username, date/time, narratives (information each individual application writes), activity type (Delete, Insert, Invalid Access, Invalid Credentials, Successful Login, Update), table name, primary key, and the application name. Auditing is performed by an ISSO. Audit logs are reviewed as least weekly, and vulnerability/compliance scanning occurs monthly.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** New users are trained in the use of PVDB.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to

reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The key privacy controls are as follows:

- User access is role-based. Not all users have access to all data.
- PVDB is housed in an off-site data center. Users and administrators access PVDB remotely from an FBINet workstation, as configured via the firewall and authentication server.
- FBI personnel receive annual privacy and information assurance training to prevent the misuse of personally identifiable information (PII).
- User groups are established by PVDB management based on a defined need to know and a role that requires access to the data.
- User accounts are disabled immediately when PVDB personnel are no longer actively employed by the program or are found to be using information inappropriately.
- SSNs are masked on reports.

In addition, as previously discussed, the system has audit capabilities via CATFOX. The following events are tracked:

- Successful and unsuccessful logon attempts;
- Starting for user access to the system;
- Failed logon attempts;
- Inactive users; and
- The record id of the information that was added, changed or deleted.

The consequences of a negative audit finding include revocation of access. The audit features are fully documented in the System Security Plan (SSP).

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

PVDB audit logs are uploaded to CATFOX and retained pursuant to National Archives and Records Administration (NARA) Job Number N1-065-10-39. Otherwise, PVDB data is temporary data and, pursuant to NARA General Records Schedule 2.2, Item 091, may be destroyed when superseded or obsolete (for registers and lists of agency personnel who have official passports), or upon the sooner of employee separation, transfer, or when 3 years old (for records related to passport and visa applications and application administration).

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained

in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X__ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

The FBI Central Records System, JUSTICE/FBI-002, 63 Fed. Reg. 8671 (Feb. 20 1998), as amended; *DOJ Computer Systems Activity and Access Records*, DOJ-002, 64 Fed. Reg. 73785 (Dec. 30, 1999), as amended.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The type, quantity, and sources of information collected and used by PVDB are necessary to obtain official and diplomatic passports and visas for FBI personnel and qualifying family members.

- The privacy risks associated with the collection and maintenance of PVDB information are inaccurate information, unauthorized access, and unauthorized disclosures.
- The privacy risks associated with the access and use of PVDB information are unauthorized access, unauthorized (or overly broad) disclosures, and loss of data.
- The privacy risks associated with the dissemination of PVDB information are the risks of unauthorized disclosures and loss of data.

These risks are mitigated generally by the controls set forth in Section 6.2. The risk of inaccurate information is further mitigated by the fact the FBI personnel data in PVDB is self-reported and can be self- amended or deleted. The risk of unauthorized access is further mitigated by the fact that only FBI employees, contractors and detailees involved in the administration of official passports and visas can access PVDB, and the information in PVDB, while broad, is narrower than the DoS passport information set. The risk of unauthorized disclosures is further mitigated by the fact that PVDB information is only shared with individuals responsible for approving or recording the issuance of official passports and visas. The risk of loss of data is further mitigated by the fact that PVDB can only be accessed within FBI-controlled space.