

# **Privacy Impact Assessment for PDVS**

## **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: Partners and Donors Vetting System
- (b) Bureau: S/GP
- (c) System acronym: PDVS
- (d) iMatrix Asset ID Number: 216087
- (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](mailto:IASolutionCenter@state.gov) for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?  
In Development
- (c) Describe the purpose of the system:  
The Partners and Donors Vetting System (PDVS) is a request submission portal for offices and missions of the U.S. Department of State. It is a tracking mechanism for the Vetting Unit's background checks on for-profit companies, non-profit organizations, civil society, and individuals. The purpose of the background check is to assist the requesting bureau or office in determining whether there are any conflicts, the appearance of conflicts, or information that could harm the reputation of the Department, which should be considered by the partnering or soliciting bureau/office, or raised to the attention of the Under Secretary for Management.

A vetting report is required for partnership partners, in-kind gift donors (support, services, goods), and cash donors in solicitation. Each report is pre-decisional, deliberative, and informational in nature to prepare an action memorandum to the Under Secretary.

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

Full name, date of birth, and mailing/residence address of individuals.

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

22 U.S.C. 2621, 22 U.S.C. 2625, Foreign Service Buildings Act of 1926, Sec. 9, as amended (22 U.S.C. 300), State Department Basic Authorities Act of 1956, Sec. 25, as amended (22 U.S.C. 2697), Foreign Assistance Act of 1961, Sec. 695(d), as amended (22 U.S.C. 2395(d)), Migration and Refugee Assistance Act of 1962, Sec. 3(a)(2), as amended (22 U.S.C. 2602), Foreign Gifts and Decorations Act, as amended (5 U.S.C. 7342 and 22 CFR part 3) Acceptance of travel and related expense from non-Federal Sources (31 U.S.C. 1353) Mutual Educational and Cultural Exchange Act of 1961 (Fulbright-Hays), Sec. 105(f) and Sec. 108A, as amended (22 U.S.C. 2455(f) and 22 U.S.C. 2458(a)) 41 CFR parts 301 and 41 CFR part 304.

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

Yes, provide:

- SORN Name and Number: Official Gift Records and Gift Donor Vetting Records, State-80
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): May 28, 2015

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](mailto: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](mailto:records@state.gov).)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): TBD
- Length of time the information is retained in the system: TBD
- Type of information retained in the system:

The Records Office is in the process of submitting the proposed schedule for review.

#### **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
- Not requested for collection

- If yes, under what authorization?

(c) How is the information collected?

Officials and missions collect the information verbally or through email from the individuals and enter the information into data fields in an online application form

(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?

It is the responsibility of the requesting office or mission that the information provided is accurate.

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

The information is accurate at the time it is entered into the system. There is no procedure or steps in place to ensure that the information remains current.

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

Not applicable. The Vetting Unit uses the information as requested by offices and missions as well as publicly available information.

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

The Vetting Unit will provide the requesting office or mission an approved Privacy Act statement in the event individual donors request the notice.

(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?

They do not provide the information to the requesting official or office.

- 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?  
PDVS only requests the minimal amount of information limited to full name, DOB, and mailing address to minimize the potential risk of harm.

**5. Use of information**

- (a) What is/are the intended use(s) for the information?  
The information is used by the vetting unit to determine whether there are any conflicts, the appearance of conflicts, or information that could harm the reputation of the Department—otherwise known as due diligence. The findings are included in due diligence reports on the individual or entity under consideration to become a partner or donor. The due diligence/vetting report is to assist the requesting bureau or office in its decision to accept the individual or entity or to raise to the attention of the Under Secretary for Management, who has the designated authority to approve or disapprove of all partners and donors.
- (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. Producing reports requires the collection, management, and tracking of the information efficiently and in an organized manner.
- (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?
  - (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.  
Information is shared with the M bureau. There is no external sharing of information.
- (b) What information will be shared?  
An individual’s full name, date of birth, and address of residence.
- (c) What is the purpose for sharing the information?  
For approval to engage with the individual or entity.

- (d) The information to be shared is transmitted or disclosed by what methods?  
The information is stored in the system, which only Vetting Unit members can log on to and access.
- (e) What safeguards are in place for each internal or external sharing arrangement?  
PDVS is safeguarded by employing secure transmission methods permitted under DoS policy for handling and transmission of sensitive but unclassified information.
- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?  
None. Information does not leave the Department's secure network.

## **7. Redress and Notification**

- (a) What procedures allow individuals to gain access to their information?  
Individuals who have cause to believe that the Official Gift Records and Gift Donor Vetting Records System may contain records pertaining to him or her can write to the Director of Office of Information Programs and Services (A/GIS/IPS) as announced through Official Gift Records and Gift Donor Vetting Records, State-80.
- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?  
 Yes    No  
  
If yes, explain the procedures.  
If an individual seeks their record by the aforementioned process and identifies any factual inaccuracies, the Vetting Unit will verify the accurate information to correct the record.  
If no, explain why not.
- (c) By what means are individuals notified of the procedures to correct their information?  
Notice of the procedure is published in State-80.

## **8. Security Controls**

- (a) How is the information in the system secured?  
  
The PDVS system is secured by the OpenNet configuration of VPN (Virtual Private Network) lines which encrypt transactions traversing the OpenNet and by role based access and privileges for users. We are currently working with IRM and the other Bureaus to identify an enterprise solution for data at rest encryption for the OpenNet.
- (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.  
  
Access to PDVS is limited to authorized DoS government and contractor employees who have a need for access to the system. All users maintain a security clearance level at least

commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network.

Each authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes rules of behavior describing the individual responsibility to safeguard information and prohibit activities (e.g., curiosity browsing).

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

Activity by authorized users is monitored, logged, and audited in accordance with US Department of State Diplomatic Security configuration guidelines at the database and server level. The system and database administrators are located in CGFS/EX and are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within PDVS are enforced by user profiles according to the principles of least privilege and separation of duties. All access to PDVS is logged by the operating system and/or the application, depending on the activities being performed.

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

Every user must attend a security briefing prior to receiving access to the DoS networks and getting a badge for facility access. This briefing also includes information regarding the Privacy Act of 1974. Users must complete initial and annual cybersecurity awareness training. The training consists of computer security awareness to include the proper handling of PII.

(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.

- **Restricted PDVS Access**

Only authorized users will have access to the system.

- **To maintain access, annual training required**

Every user must attend a security briefing to receive access to the DoS networks. Subsequently, all PDVS users must complete annual cybersecurity and privacy training to maintain their PDVS access.

- **Roles & Permissions within the PDVS application**

All rights to information and functionality within PDVS are enforced by user profiles to limit access according to the principles of least privilege and separation of duties.

- **PDVS has single sign on**

PDVS users will not be able to log onto another user's PDVS account while logged onto the DoS network under their credentials.

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

Information does not leave the Vetting Unit once submitted into the system by Department offices and missions. However, sensitive information is required to be collected. The security measures were designed to minimize privacy risks without hampering necessary business operations of the State Department.

## **9. Data Access**

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

The Vetting Unit, who are the only authorized users, have access to the system. Access to PDVS is limited to authorized DoS government and contractor employees who have a need for access to the system. All users maintain a security clearance level at least commensurate with public trust positions.

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

Users must be members of the Vetting Unit and conducting due diligence assessments to be granted access.

- (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.

Access is restricted to all users in the Vetting Unit.

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

Before the Vetting Unit uses an individual's information for due diligence, Lexis Nexis and the Branch Chief, Information Resources under the Bureau of Administration/Global Information Services/Information Programs and Services are contacted and made aware of the search of the individual on Vetting Unit member computer stations; the subscription for Lexis Nexis is hosted by Information Resources. Also, activity by authorized users is monitored, logged, and audited in accordance with US Department of State Diplomatic Security configuration guidelines at the database and server level. The system and database administrators are located in CGFS/EX and are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within PDVS are enforced by user profiles according to the principles of least privilege and separation of duties. All access to PDVS is logged by the operating system and/or the application, depending on the activities being performed.