Partner Vetting System (PVS) Privacy Impact Assessment (PIA)

UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

Office of the Chief Information Officer (M/CIO)
Information Assurance Division
Partner Vetting System (PVS)
Approved Date: January 17, 2017

Additional Privacy Compliance Documentation Required:

☐ None

☒ System of Records Notice (SORN)

☐ Open Data Privacy Analysis (ODPA)

☐ Privacy Act Section (e)(3) Statement or Notice (PA Notice)

☐ USAID Web Site Privacy Policy

☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents

☐ Role-Based Privacy Training Confirmation

Possible Additional Compliance Documentation Required:

☐ USAID Forms Management. ADS 505

☐ Information Collection Request (ICR). ADS 505, ADS 506, and ADS 508 Privacy Program

☐ Records Schedule Approved by the National Archives and Records Administration. ADS 502

Table of Contents

1 Introduction

The USAID Privacy Office is using this Privacy Impact Assessment (PIA) Template to gather information from program managers, system owners, and information system security officers in order to analyze USAID information technology and information collections (systems) that collect, use, maintain, or disseminate personally identifiable information (PII). See **ADS 508 Privacy Program** Section 503.3.5.2 Privacy Impact Assessments.

2 Information

2.1 Program and System Information

2.1.1 Describe the PROGRAM and its PURPOSE.

The United States Agency for International Development (USAID) is the lead U.S. Government agency that works to end extreme global poverty and enable resilient, democratic societies to realize their potential. The USAID mission states: We partner to end extreme poverty and promote resilient, democratic societies while advancing our security and prosperity.

USAID's Partner Vetting System (PVS) is owned and operated by the Office of Security (SEC), Counterterrorism and Information Security Division (SEC/CTIS). This division is responsible for the following tasks:

- Developing policies and procedures for USAID regarding the screening of USAID's implementing partners for terrorism ties;
- Managing the counterintelligence, classified national security information, and national industrial security programs;
- Overseeing the handling and storage of classified information; and

Implementing an Agency inspection program for storage of classified national security information.

2.1.2 Describe the SYSTEM and its PURPOSE.

The mission of PVS is to ensure that no government dollars fall into the hands of terrorists, terrorist organizations, or individuals/groups who support terrorist activities. The data submitted by the partners is used to identify a specific individual so that a screening can be performed. Potential or current USAID implementing partners use PVS to submit information to USAID about their organizations, subcontractors, and an organization's principals so that USAID can vet these groups.

PVS is a database that supports the vetting of directors, officers, or other employees of non-governmental organizations who apply for USAID contracts, grants, cooperative agreements, or other funding and those who apply for registration with USAID as Private and Voluntary Organizations. The information collected from the individuals is specifically used to conduct screening to ensure that USAID funds and USAID-funded activities are not purposefully or inadvertently used to provide support to entities or individuals deemed to be a risk to the national security of the United States of America. Specifically, PVS is used to uniquely identify an individual whose data is submitted into the system; it is not used to conduct an investigation in regard to a specific individual.

PVS is a USAID major application that is hosted within the USAID Intranet. There are approximately 90 users located in Tel Aviv, Israel, and USAID Washington (USAID/W). PVS currently does not support users external to the Agency. The application has an external-facing website that is used by partner organizations to enter their data. The servers hosting the application conform to USAID standard policies. The only transactions that are conducted over the Internet are potential partners submit their data. The web interface is located in USAID's DMZ and allows

2.1.2 Describe the SYSTEM and its PURPOSE.

USAID partners to access a portion of the system to enter their data directly. All transactions performed by USAID personnel are carried out within the USAID network (AIDNET). This system is connected to AIDNET and is accessed by SEC and Mission users through a Web-based interface.

Note that PVS is not a national security system and bears a FIPS-199 risk level of "moderate." None of the information types present in PVS are rated as "high."

2.1.3 What is the SYSTEM STATUS?

☐ New System Development or Procurement

☐ Pilot Project for New System Development or Procurement

☒ Existing System Being Updated

☐ Existing Information Collection Form or Survey
OMB Control Number:

☐ New Information Collection Form or Survey

☐ Request for Dataset to be Published on an External Website

☐ Other:

2.1.4 What types of INFORMATION FORMATS are involved with the program?

☐ Physical only

☐ Electronic only

☒ Physical and electronic combined: USAID Form 500-13 may be submitted online or completed by hand. The physical, handwritten documents are not retained; however, all copies of the form are stored online. PVS staff (Vetting Support Unit), whether at the mission site or at the Washington, DC Bureau intakes the physical forms from potential partners and inputs the data manually into PVS. Once complete, the forms are shredded by the PVS staff members compliant with Records Management (within 5 years). Five years is the maximum time these records can be maintained. Individual missions, however, dispose of the forms different intervals. While being stored, paper copies are maintained in locked filing cabinets. OMB confirmed the disposition schedule for hardcopy USAID Forms 500-13 should be the Electronic Disposition Schedule under ADS 502maa.

2.1.5 Does your program participate in PUBLIC ENGAGEMENT?

☒ No. PVS engages with specific individuals who have an established or are seeking a certain relationship with USAID. This system does not allow for access by or collect information from the public in general. Information may be collected on individuals working within the companies seeking to partner with the Agency.

☐ Yes:

- ☐ Information Collection Forms or Surveys
- ☐ Third Party Web Site or Application
- ☐ Collaboration Tool

2.1.6 What type of system and/or TECHNOLOGY is involved?
☐ Infrastructure System (Local Area Network, Wide Area Network, General Support System, etc.)
☒ Network: AIDNET
☒ Database
☒ Software
☐ Hardware
☐ Mobile Application or Platform [Note: PVS can be accessed from any web-enabled device, but it does not have a dedicated design for mobile usage. There is no application for PVS, for example.]
☐ Mobile Device Hardware (cameras, microphones, etc.)
☐ Quick Response (QR) Code (matrix geometric barcodes scanned by mobile devices)
☐ Wireless Network
☐ Social Media
☒ Web Site or Application Used for Collaboration with the Public
☐ Advertising Platform
☐ Website or Webserver
☐ Web Application
☐ Third-Party Website or Application
☐ Geotagging (locational data embedded in photos and videos)
☐ Near Field Communications (NFC) (wireless communication where mobile devices connect without contact)
☐ Augmented Reality Devices (wearable computers, such as glasses or mobile devices, that augment perception)
☐ Facial Recognition
☐ Identity Authentication and Management
☐ Smart Grid
☐ Biometric Devices
☐ Bring Your Own Device (BYOD)
☐ Remote, Shared Data Storage and Processing (cloud computing services)
☐ Other:
☐ None

2.1.7 About what types of people do you collect, use, maintain, or disseminate personal information?
☒ Citizens of the United States
☒ Aliens lawfully admitted to the United States for permanent residence
☒ USAID employees and personal services contractors
☒ Employees of USAID contractors and/or services providers
☒ Aliens
☒ Business Owners or Executives
☒ Others: Potential grant awardees (and their employees) (who could be US citizens or foreign nationals) [Note: The PVS database may have data about USAID employees, PSCs, contractors, and other service providers, but such data's presence is coincidental as it is not the target of PVS.]
☐ None

2.2 Information Collection, Use, Maintenance, and Dissemination

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☒ Name, Former Name, or Alias
☐ Mother's Maiden Name
☒ Social Security Number or Truncated SSN
☒ Date of Birth
☒ Place of Birth
☒ Home Address
☒ Home Phone Number
☒ Personal Cell Phone Number
☒ Personal E-Mail Address
☒ Work Phone Number
☒ Work E-Mail Address
☒ Driver's License Number
☒ Passport Number or Green Card Number
☒ Employee Number or Other Employee Identifier
☐ Tax Identification Number

2.2.1 What types of personal information do you collect, use, maintain, or disseminate?
☐ Credit Card Number or Other Financial Account Number
☐ Patient Identification Number
☒ Employment or Salary Record
☐ Medical Record
☐ Criminal Record
☐ Military Record
☐ Financial Record
☐ Education Record
☒ Biometric Record (signature, fingerprint, photo, voice print, physical movement, DNA marker, retinal scan, etc.)
☒ Sex or Gender
☒ Age
☐ Other Physical Characteristic (eye color, hair color, height, tattoo)
☐ Sexual Orientation
☐ Marital status or Family Information
☐ Race or Ethnicity
☐ Religion
☒ Citizenship
☒ Other:
☐ No PII is collected, used, maintained, or disseminated

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☒ Log Data (IP address, time, date, referrer site, browser type)
☒ Tracking Data (single- or multi-session cookies, beacons)
☒ Form Data
☒ User Names
☐ Passwords
☐ Unique Device Identifier
☐ Location or GPS Data

2.2.2 What types of digital or mobile data do you collect, use, maintain, or disseminate?
☐ Camera Controls (photo, video, videoconference)
☐ Microphone Controls
☐ Other Hardware or Software Controls
☒ Photo Data: [Note: Photos can be uploaded but are not requested. Photo collection is not mandatory and PVS submissions can be completed without uploading photos.]
☐ Audio or Sound Data
☐ Other Device Sensor Controls or Data
☐ On/Off Status and Controls
☐ Cell Tower Records (logs, user location, time, date)
☐ Data Collected by Apps (itemize)
☐ Contact List and Directories
☐ Biometric Data or Related Data
☐ SD Card or Other Stored Data
☐ Network Status
☐ Network Communications Data
☐ Device Settings or Preferences (security, sharing, status)
☐ Other:
☐ None

2.2.4 Who owns and/or controls the system involved?
☒ USAID Office: USAID/SEC/CTIS
☐ Another Federal Agency:
☐ Contractor:
☐ Cloud Computing Services Provider:
☐ Third-Party Website or Application Services Provider:
☐ Mobile Services Provider:
☐ Digital Collaboration Tools or Services Provider:
☐ Other:

3 Privacy Risks and Controls

3.1 Authority and Purpose (AP)

3.1.1 What are the statutes or other LEGAL AUTHORITIES that permit you to collect, use, maintain, or disseminate personal information?

Since September 2001, Executive Order 13224 has prohibited any transactions or dealings with entities or individuals designated as terrorists; Since Fiscal Year 2003, the annual foreign operations appropriations legislation (Section 559) has required that, ‘‘the Secretary of State shall take all appropriate steps to ensure that such assistance is not provided to or through any individual, private or government entity, or education institution that the Secretary knows or has reason to believe advocates, plans, sponsors, engages in, or has engaged in, terrorist activity.

18 U.S.C. 2339A, 2339B, 2339C; 22 U.S.C. 2151 et seq.; Section 559 of FY06 Foreign Operations Appropriations Act; Executive Orders 13224, 13099 and 12947; and HSPD-6.

PVS-maintained PII can be shared with the FBI Terrorist Screening Center (TSC) only when there is a positive match between an individual in the PVS database and the TSC database. USAID and FBI manage this data sharing relationship through an MOU. Authorities for the MOU are provided therein.

3.1.2 Why is the PII collected and how do you use it?

USAID collects the PII requested on USAID Form 500-13 in order to support vetting of directors, officers, or other employees of non-governmental organizations who apply for USAID contracts, grants, cooperative agreements, or other funding, and those applying for registration with USAID as Private and Voluntary Organizations. The information collected from the individuals is specifically used to conduct screening to ensure that USAID funds and USAID-funded activities are not purposefully or inadvertently used to provide support to entities or individuals deemed to be a risk to the national security of the United States of America.

3.1.3 How will you identify and evaluate any possible new uses of the PII?

The following is an informal process employed by the SEC office: Any potential new uses of the data would be brought to the attention of the Director of Management Policy, Budget and Performance (M/MPBP) for evaluation of the merits of the proposed new use. If the use is considered worthwhile, the M/MPBP Director would then consult with USAID General Counsel and the Privacy Program to evaluate legal and privacy concerns. Outside of this process, SEC adheres to USAID’s M/CIO change control process.

3.2 Accountability, Audit, and Risk Management (AR)

3.2.1 Do you use any data collection forms or surveys?

☐ No:

☒ Yes:

- ☒ Form or Survey (Please attach)
- ☐ OMB Number, if applicable:
- ☐ Privacy Act Statement (Please provide link or attach PA Statement)

3.2.3 Who owns and/or controls the personal information?

☒ USAID Office: USAID Office of Security [Note: USAID owns all data within the system, which is maintained on virtualized servers.]

☐ Another Federal Agency:

☐ Contractor:

☐ Cloud Computing Services Provider:

☐ Third-Party Web Services Provider:

☐ Mobile Services Provider:

☐ Digital Collaboration Tools or Services Provider:

☐ Other:

3.2.8 Do you collect PII for an exclusively statistical purpose? If you do, how do you ensure that the PII is not disclosed or used inappropriately?

☒ No.

☐ Yes:

3.3 Data Quality and Integrity (DI)

3.3.1 How do you ensure that you collect PII to the greatest extent possible directly from the subject individual?

All PII information is collected directly from the individual or group who is requesting USAID funding assistance. The retrieval of this information is digital and is maintained in the PVS system. Information can be edited directly in the system through the Partner Information Form (PIF) which is a form within the system used to collect data.

3.3.2 How do you ensure, to the greatest extent possible, that the PII is accurate, relevant, timely, and complete at the time of collection?

All PII that is entered is validated by internal controls in the PVS application program interface (API). Validation of addresses includes using automated verification look-up. While every attempt is made to validate information electronically, manual validation is also used to maintain accuracy and integrity of the data presented. The partners enter the data directly and can also search PVS for records they have already submitted to ensure that they are accurate.

3.3.3 How do you check for, and correct as necessary, any inaccurate or outdated PII in the system?

Individuals requesting amendment of their record(s) maintained by USAID must identify the information to be changed and the corrective action sought. Requests must follow the "Contesting Record and Record Access Procedures" section in SORN USAID-027: "United States citizens or legal permanent residents can request access to a non-exempt record pertaining to him/her by sending a request in writing, signed, to the Chief Privacy Officer at the following address: Chief Privacy Officer, United States Agency for International Development, 1300 Pennsylvania Avenue, NW., Office 2.12–003, Washington, DC 20523–2120."
PVS staff does not review and reach out to the individual submitter should it appear incorrect. However, partners can directly access PVS through the NGO Portal and update previously submitted PII by submitting a new USAID Form 500-13 (PIF). Replacement PIFs are reviewed by a vetting analyst before they are uploaded into PVS and, should the information appear correct, the Vetting Official then ensures the data was entered correctly or work with the partner to make additional corrections.

3.4 Data Minimization and Retention (DM)

3.4.1 What is the minimum PII relevant and necessary to accomplish the legal purpose of the program?

Name, address, date of birth, place of birth, and citizenship are required to commence an investigation. Additional elements listed on Form 500-13 are collected, and this additional information is required to ensure accuracy and timeliness during the vetting process, which is carried out to validate that USAID funding assistance does not provide support to individuals or entities associated with terrorism.

Some individuals whose personal information is collected by PVS are foreign nationals. Identifying a person with the precision required for PVS can be difficult depending on the country they are from. While the items listed in this section are the minimum needed, other data elements may sometimes be needed because of how other countries identify people.

3.4.3 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected? Is the PII relevant and necessary to the specified purposes and how is it maintained?

☐ No.

☒ Yes: Determinations regarding whether the applicant can receive a USAID Grant, contract, cooperative agreement, or other funding.

3.4.4 What types of reports about individuals can you produce from the system?

There are two types of reports that can be run: Individual (Beneficiaries) and Key Individual (Key members of Partner). The purpose of the reports is to deliver quality control in the system and to show how many people have been vetted based on a particular criteria (e.g., by a particular Mission). The only information that is presented in the report is a list names that meet the search criteria and their citizenship, vetting start and end date, and the vetting result. Vetting Officials, vetting assistants, system administrator, and vetting analyst can run and view the report. This report is used to generate statistical information (no personal information included) regarding vetting activity that is used to show vetting statistics to a Mission Front Office. Information included is the number of vettings that have completed and what were the final determinations (eligible or ineligible).

3.4.6 Does the system monitor or track individuals?

(If you choose Yes*, please explain the monitoring capability.)*

☒ No.

☐ Yes:

3.5 Individual Participation and Redress (IP)

3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?

Individuals who access PVS are given the opportunity to enter their PII; they can choose to not participate. Potential submitters receive the following message in English when accessing the PVS Portal website:

Thank you for visiting the PVS Portal. Your privacy and security are very important to us. Please be aware that USAID does not collect personal information when you visit our website, unless you choose to provide that information. However, we do collect some technical information about your visit to USAID.gov. This is how we handle information about your visit to our Web site:
Information Collected and Stored Automatically
When you visit PVS Portal, we may store some or all of the following:

- the IP address from which you accessed our site
- the date and time
- the pages you visited on our site
- the browser and operating system used
- user name when logging in
- Information You Provide to USAID

USAID will only use your personal information for the purpose for which it was provided. When you voluntarily submit information, it constitutes your consent to the use of the information for the purpose stated.

3.5.1 Do you contact individuals to allow them to consent to your collection and sharing of PII?

Along with the Privacy Notice, the user is informed about the how the information is collected and how it is used to ensure that all the data entered by users is secure and is used for the purposes for which it is intended.

See https://ngoportal.usaid.gov/NGO/.

3.5.2 What mechanism do you provide for an individual to gain access to and/or to amend the PII pertaining to that individual?

Individuals requesting amendment of their own records maintained by USAID must identify the information to be changed and the corrective action sought. Requests must submit the request in writing to the Chief Privacy Officer, USAID, 1300 Pennsylvania Avenue, NW., Office 2.12–003, Washington, DC 20523–2120. The request must include the requestor's full name, his/her current address and a return address for transmitting the information. The request shall be signed by either notarized signature or by signature under penalty of perjury and reasonably specify the record contents being sought. USAID partners who have entered information can also directly access the system through the NGO Portal interface with their username and password. They are able to directly access their information to amend their PII similar to when they entered the data originally.

Partners may also submit a new USAID Form 500-13, which would then be reviewed by the Vetting Official prior to being uploaded in the PVS database.

3.5.3 If your system involves cloud computing services and the PII is located outside of USAID, how do you ensure that the PII will be available to individuals who request access to and amendment of their PII?

Not Applicable.

3.7 Transparency (TR)

3.7.1 Do you retrieve information by personal identifiers, such as name or number?

(If you choose Yes, please provide the types of personal identifiers that are used.)

☐ No.

☒ Yes: Individual name, date of birth, place of birth, social security numbers, passport numbers or other identifying data

3.7.2 How do you provide notice to individuals regarding?

1) The authority to collect PII: SORN USAID-027

2) The principal purposes for which the PII will be used: SORN USAID-027 and Privacy Notice

3) The routine uses of the PII: SORN USAID-027 and Privacy Notice provided on login screen

4) The effects on the individual, if any, of not providing all or any part of the PII: SORN USAID-027

Each element is detailed on the final page of USAID Form 500-13.

3.7.3 Is there a Privacy Act System of Records Notice (SORN) that covers this system?

☐ No

☒ Yes: USAID-027

3.7.4 If your system involves cloud computing services, how do you ensure that you know the location of the PII and that the SORN System Location(s) section provides appropriate notice of the PII location?

Not Applicable.

3.8 Use Limitation (UL)

3.8.1 Who has access to the PII at USAID?

Access to the PVS systems is via the AIDNet Active Directory. PVS identifies account types (regular PVS web application users) and queries AIDNet's Active Directory user listing to validate USAID employees. This ensures that only employees, contractors, and other Active Directory users have access to the PVS system and, consequently, the PII data. Specific user types that have access to PII include: Partner submitter (their own), Mission Security Coordinators (access to PII of their Partners), and Vetters (access to all Partner PII). Note that the system is managed by the USAID M/CIO general O&M contractor, which is currently IBM. Historically, this data has not been encrypted, but it will be in the immediate future. SEC/CTIS/CT analysts and Intelligence Research Specialists (FSLs) funded by Bureaus access, review, and analyze PVS data and make recommendations to approve or deny applicants based on the same. They have access view each PVS record but cannot edit the records. They can view all PII information as it is required and necessary in order for them to do their job.

Outside of the FBI, who can receive PVS data shared with them through an existing MOU, only those with access to PVS within USAID can access the PII. (Note: FBI does not access the system to review the data but rather receives it from a vetter.)

3.8.3 With whom do you share the PII outside of USAID? And whether (and how, if applicable) you will be using the system or related web site or application to engage with the public?

PVS maintained PII can be shared with the FBI Terrorist Screening Center (TSC) only when there is a positive match between an individual in the PVS database and the TSC database. Vetting analysts check for the match manually and also review the data to confirm whether PVS has supplemental data no present in the TSC database. USAID and FBI manage this data sharing relationship through an MOU. FBI does not access the system to review the data but rather receives it from a vetter.

3.8.4 Do you share PII outside of USAID? If so, how do you ensure the protection of the PII 1) as it moves from USAID to the outside entity and 2) when it is used, maintained, or disseminated by the outside entity?

☐ No.

☒ Yes:

3.9 Third-Party Web Sites and Applications

3.9.1 What PII *could be made available* (even though not requested) to USAID or its contractors and service providers when engaging with the public?

Only the applicant can make PII available to USAID through explicit consent or providing the PII himself or herself. Specifically, a potential partner may upload files into PVS through the NGO Portal interface, and all uploads must be approved by the Vetting Official before they are made a part of PVS. Forms collected into PVS do have open text fields, but there is no cut-and-paste functionality, so entrants must manually enter all information into the system

Appendix A. Links and Artifacts

A.1 Privacy Compliance Documents or Links

☐ None. There are no documents or links that I need to provide.
☐ Privacy Threshold Analysis (PTA)
☐ Privacy Impact Assessment (PIA)
☐ System of Records Notice (SORN)
☐ Open Data Privacy Analysis for Posting Datasets to the Public (ODPA)
☐ Data Collection Forms or Surveys
☐ Privacy Act Section (e)(3) Statements or Notices
☐ USAID Web Site Privacy Policy
☐ Privacy Policy of Third-Party Web Site or Application
☐ Privacy Protection Language in Contracts and Other Acquisition-Related Documents