



This document is scheduled to be published in the Federal Register on 12/05/2012 and available online at <http://federalregister.gov/a/2012-29388>, and on [FDsys.gov](http://FDsys.gov)

## **AGENCY FOR INTERNATIONAL DEVELOPMENT**

### **Privacy Act of 1974; System of Records**

**AGENCY:** United States Agency for International Development.

**ACTION:** Privacy Act System of Records Notice - Altered

**SUMMARY:** Pursuant to the provisions of the Privacy Act of 1974 (5 U.S.C. 552a), the United States Agency for International Development (USAID) is giving notice that it proposes to alter a system of records, the Partner Vetting System (PVS). This system supports the vetting of individuals, officers, or other officials of nongovernmental organizations who apply for USAID contracts, grants, cooperative agreements, or other funding, or who apply for registration with USAID as Private and Voluntary Organizations (PVOs), ensuring that neither USAID funds nor USAID-funded activities inadvertently or otherwise provide support to entities or individuals associated with terrorism.

**DATES:** Public comments must be received on or before January 10, 2013. Unless comments are received that would require a further revision, this altered system of records will become effective on January 10, 2013.

**ADDRESSES:** You may submit comments to:

#### **Paper Comments:**

- Fax: (703) 666-5670
- Mail: Chief Privacy Officer, United States Agency for International Development, 2733 Crystal Drive, 11th Floor, Arlington, Va. 22202

#### **Electronic Comments:**

- Federal eRulemaking Portal: <http://www.regulations.gov>. Follow the instructions on the Web site for submitting comments.
- E-mail: [privacy@usaid.gov](mailto:privacy@usaid.gov).

**FOR FURTHER INFORMATION CONTACT:** For general questions, please contact, USAID Privacy Office, United States Agency for International Development, 2733 Crystal Drive, 11th Floor, Arlington, Va. 22202. E-mail: [privacy@usaid.gov](mailto:privacy@usaid.gov).

**SUPPLEMENTARY INFORMATION:**

USAID has established a system of records pursuant to the Privacy Act (5 U.S.C. 552a), entitled the Partner Vetting System (PVS) which includes the PVS Portal . Partner Vetting System supports the vetting of directors, officers, or other employees of non-governmental organizations who apply for USAID contract, grants, cooperative agreements or other funding, or who apply for registration with USAID as Private and Voluntary Organizations. The information collected from 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 national security.

The PVS Portal provides these organizations with secure, web-based functionality for the completion, submission and tracking of Partner Information Forms (PIF's). This information is used to conduct screening to ensure that USAID funds as well as funded activities are not purposely or inadvertently used to provide support to entities or individuals deemed to be a risk to national security.

Dated: November 22, 2012

William Morgan

Chief Information Security Officer - Chief Privacy Officer

**USAID-027**

**SYSTEM NAME:** Partner Vetting System Portal

**SECURITY CLASSIFICATION:** Classified and Sensitive but Unclassified.

**SYSTEM LOCATION:**

Terremark; 50 NE 9<sup>th</sup> Street; Miami, FL 33132

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

a. Individuals who are directors, officers, or are otherwise employed by either for-profit or non-profit nongovernmental organizations who apply for USAID contracts, grants, cooperative agreements or other types of instruments;

b. Individuals who apply for personal services contracts or for other contracts, grants, or cooperative agreements;

c. Individuals or organizations who attempt to obtain other USAID assistance or benefits;

d. Individuals who are officers or other officials of non-profit, nongovernmental organizations who apply for registration with USAID as Private and Voluntary Organizations (PVOs).

**CATEGORIES OF RECORDS IN THE SYSTEM:**

*Sensitive but Unclassified and nonexempt identifying information in this system includes, but is not limited to:*

- Full name (including any aliases or variations of spelling),
- Date and place of birth,

- Government-issued identification information (including, but not limited to, social security number, passport number, or other numbers originated by a government that specifically identifies an individual),
- Current mailing address,
- Telephone and fax numbers,
- Email addresses,
- Country of origin and/or nationality,
- Citizenship,
- Gender, and
- Profession or other employment data.

*Classified and exempt information in this system includes, but is not limited to:*

- Results generated from the screening of individuals covered by this notice;
- Intelligence and law enforcement information related to national security; and
- National security vetting and terrorism screening information, provided to USAID by other agencies.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

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.

**PURPOSE(S):**

To support the vetting of directors, officers, or other employees of nongovernmental organizations who apply for USAID contracts, grants, cooperative agreements or other funding or who apply for registration with USAID as Private and

Voluntary Organizations. The information collected from these 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 national security.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

USAID may disclose relevant system records in accordance with any current and future blanket routine uses established for its record systems. See the Statement of General Routine Uses (and amendments), 42 FR 47371 (September 20, 1977); 59 FR 52954 (October 20, 1994); 59 FR 62747 (December 6, 1994). Routine uses are not meant to be mutually exclusive and may overlap in some cases.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, PROTECTING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:  
STORAGE:**

Records in this system are stored in both paper and electronic format. Paper records are maintained by the USAID regional offices when the information cannot be collected electronically. Electronic storage is on servers (hard disk media) and magnetic tapes (or other backup media).

**RETRIEVABILITY:**

Records in this system are retrieved by individual name, date of birth, place of birth, social security numbers, passport numbers or other identifying data specified under Categories of Records in the System.

**SAFEGUARDS:**

USAID maintains all classified records in an authorized security container with access limited to authorized government personnel and authorized contractors. Physical security protections include guards and locked facilities requiring badges. Only authorized government personnel and authorized contractors can access records within the system. USAID mandates and certifies that physical and technological safeguards appropriate for classified and Sensitive but Unclassified systems are used to protect the records against unauthorized access. All authorized government personnel and authorized contractors with access to the system must hold appropriate security clearance, sign a non-disclosure agreement, and undergo both privacy and security training.

*For paper records:* Classified and Sensitive but Unclassified records are kept in an approved security container at the USAID Washington headquarters, and at the relevant location(s) where USAID has a program. Access to these records is limited to those authorized government personnel and authorized contractors who have a need for the records in the performance of their official duties.

*For electronic records:* Records are kept in a secure database in the USAID Washington headquarters. Access to the records is restricted to those authorized government personnel and authorized contractors with a specific role in the vetting process as part of the performance of their official duties. The PVS database is housed on and accessed from a Sensitive but Unclassified computer network. Vetting requests, analyses, and

results will be stored separately on a classified computer network. Both computer networks and the PVS database require a user identification name and password and approval from the Office of Security. An audit trail is maintained and periodically reviewed to monitor access to the system. Authorized government personnel and authorized contractors assigned roles in the vetting process are provided role-specific training to ensure that they are knowledgeable in how to protect personally identifiable information.

**RETENTION AND DISPOSAL:**

Records in this system will be retained and disposed of in accordance with a records schedule approved by the National Archives and Records Administration.

**SYSTEM MANAGER(S) AND ADDRESS:**

Chief, Counterterrorism and Information Security Division , Office of Security, United States Agency for International Development, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW., Washington, DC 20523.

**NOTIFICATION PROCEDURE:**

Individuals requesting notification of the existence of records on them must send the request in writing to the Chief Privacy Officer, USAID, 2733 Crystal Drive, 11th Floor, Arlington, Va. 22202. 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.

This system contains classified information related to the government's national security programs, records in this system may be exempt from notification, access, and amendment as permitted by subsection (j) and (k) of the Privacy Act.

**RECORD ACCESS PROCEDURES:**

Requests from individuals should be addressed or presented in person to the same addresses as stated in the Notification Section above. Requests should be accompanied by information sufficient to identify the individual pursuant to Sec. 215.4(c) or (d) of the Agency's Regulations as published in this issue of the Federal Register.

**CONTESTING RECORD PROCEDURES:**

An individual requesting amendment of a record maintained on himself or herself must identify the information to be changed and the corrective action sought. Requests must follow the "Notification Procedures" above.

**RECORD SOURCE CATEGORIES:**

Information in this system is obtained from the non-governmental organization's official who is responsible for completing the application package required to compete for USAID funds or who apply for registration with USAID as a Private and Voluntary Organization. In the case of applications by an individual in his/her own capacity, the information will be collected directly from the individual applicant. Information in this system may also be obtained from public sources, agencies conducting national security screening, law enforcement and intelligence agency record systems, and other government databases.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

22 CFR Part 215, Section 215.13 General Exemptions:

(c) The systems of records to be exempted under section (j)(2) of the Act, the provisions of the Act from which they are being exempted, and the justification for the exemptions, are set forth below:

(2) Partner Vetting System. This system is exempt from sections (c)(3) and (4); (d); (e)(1), (2), and (3); (e)(4)(G), (H), and (I); (e)(5) and (8); (f), (g), and (h) of 5 U.S.C. 552a. These exemptions are necessary to insure the proper functioning of the law enforcement activity, to protect confidential sources of information, to fulfill promises of confidentiality, to maintain the integrity of law enforcement procedures, to avoid premature disclosure of the knowledge of criminal activity and the evidentiary basis of possible enforcement actions, to prevent interference with law enforcement proceeding, to avoid the disclosure of investigative techniques, to avoid endangering law enforcement personnel, to maintain the ability to obtain candid and necessary information, to fulfill commitments made to sources to protect the confidentiality of information, to avoid endangering these sources, and to facilitate proper selection or continuance of the best applicants or persons for a given position or contract. Although the primary functions of USAID are not of a law enforcement nature, the mandate to ensure USAID funding is not purposefully or inadvertently used to provide support to entities or individuals deemed to be a risk to national security necessarily requires coordination with law enforcement and intelligence agencies as well as use of their information. Use of these agencies' information necessitates the conveyance of these other systems exemptions to protect the information as stated. [57 FR 38277, Aug. 24, 1992, as amended at 74 FR 16, Jan. 2, 2009]

22 CFR 215.14 - Specific Exemptions.

(c) The systems of records to be exempted under section (k) of the Act, the provisions of the Act from which they are being exempted, and the justification for the exemptions, are set forth below:

(6) Partner Vetting System. This system is exempt under *5 U.S.C. 552a* (k)(1), (k)(2), and (k)(5) from the provision of *5 U.S.C. 552a* (c)(3); (d); (e)(1); (e)(4)(G), (H), (I); and (f). These exemptions are claimed to protect the materials required by executive order to be kept secret in the interest of national defense or foreign policy, to prevent subjects of investigation from frustrating the investigatory process, to insure the proper functioning and integrity of law enforcement activities, to prevent disclosure of investigative techniques, to maintain the ability to obtain candid and necessary information, to fulfill commitments made to sources to protect the confidentiality of information, to avoid endangering these sources, and to facilitate proper selection or continuance of the best applicants or persons for a given position or contract. [57 FR 38277, Aug. 24, 1992, as amended at 74 FR 17, Jan. 2, 2009]

---

Meredith Snee  
Privacy Analyst

[FR Doc. 2012-29388 Filed 12/04/2012 at 8:45 am; Publication Date: 12/05/2012]