6116-01-M

AGENCY FOR INTERNATIONAL DEVELOPMENT

Privacy Act of 1974, System of Records

AGENCY: United States Agency for International Development

ACTION: Altered system of records.

SUMMARY: The United States Agency for International Development (USAID) is issuing public notice of its intent to alter a system of records maintained in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), as amended, entitled "USAID-09, Criminal Law Enforcement Records System". USAID is updating this system of record for a non-significant change, to reflect the address change for the location of the system. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of record systems maintained by the agency (5 U.S.C. 522a(e)(4)).

DATES: The 30-day public comment period and 10-day additional OMB and Congress review period is not required for non-significant alterations.

ADDRESSES: You may submit comments:

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.

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.

SUPPLEMENTARY INFORMATION: The Criminal Law Enforcement Records System, will now be electronically stored and located in a new location. The new location is: Terremark NAP of the Americas, 2 S Biscayne Blvd Miami FL 33131.

Dated: March 15, 2013.

William Morgan

Chief Information Security Officer - Chief Privacy Officer

USAID-09

System Name: Criminal Law Enforcement Records System

Security Classification: Sensitive But Unclassified.

System location: Terremark NAP of the Americas, 2 S Biscayne Blvd Miami FL 33131

Categories of individuals covered by the system: In connection with its investigative duties, OIG maintains records in its Criminal law Enforcement Records System on the following categories of individuals insofar as they are relevant to any investigation or preliminary inquiry undertaken to determine whether to commence an investigation: complainants; witnesses; confidential and non-confidential informants; contractors; subcontractors; recipients of federal assistance or funds and their contractors/subcontractors and employees; individuals threatening USAID employees or the USAID Administrator; current, former, and prospective employees of USAID; alleged violators of USAID rules and regulations; union officials; individuals investigated and/or interviewed; persons suspected of violations of administrative, civil, and/or criminal provisions; grantees,' sub-grantees; lessees; licensees; and other persons engaged in official business with USAID.

Categories of records covered by this system: The system contains investigative reports and materials gathered or created with regard to investigations of administrative, civil, and criminal matters by OIG and other Federal, State, local, tribal, territorial, or foreign regulatory or

law enforcement agencies. Categories of records may include: complaints; request to investigate; information contained in criminal, civil, or administrative referrals; statements from subjects, targets, and /or witnesses; affidavits, transcripts, police reports, photographs, and/or documents relative to a subject's prior criminal record; medical records, accident reports, materials and intelligence information from other governmental investigatory or law enforcement organizations; information relative to the status of a particular complaint or investigation, including any determination relative to criminal prosecution, civil, or administrative action; general case management documentation' subpoenas and evidence obtained in response to subpoenas; evidence logs; pen registers; correspondence, records of seized property' reports of laboratory examination; reports of investigation; and other data or evidence collected or generated by OIG's Office of Investigations during the course of conducting its official duties.

Authority for maintenance of the system: The Inspector General Act of 1978, 5 U.S.C. App. 3, as amended.

Purpose(s): The records contained in this system are used by OIG to carry out its statutory responsibilities under the Inspector General Act of 1978, as amended, to conduct and supervise investigations relating to programs and operations of USAID; to promote economy, efficiency, and effectiveness in the administration of such programs and operations; and to prevent and detect fraud, waste, and abuse in such programs and operations. The records are used in the course of investigating individuals and entities suspected of having committed illegal or unethical acts, and in conducting related criminal prosecutions, civil proceedings, and administrative actions.

Routine use of records maintained in the system, including categories of users and the purpose of such uses: USAID's routine uses, see 42 FR 47371 (September 20, 1977) and 59 FR 52954 (October 20, 1994), apply to this system of records. As additional routine uses for this records system, USAID/OIG may disclose information in this system as follows:

(a) Disclosure to the Department of Justice (DOJ) or a legal representative designated by a Federal Agency in circumstances in which:

(1) USAID or OIG, or any component thereof:

(2) Any employee of USAID or OIG in his or her official capacity;

(3) Any employee of USAID or OIG in his or her individual capacity, where the DOJ has agreed to represent or is considering a request to represent the employee; or

(4) The United States or any of its components is a party to pending or potential litigation or has an interest in such litigation, USAID or OIG will be affected by the litigation, or USAID or OIG determines that the use of such records by the DOJ is relevant and necessary to the litigation; provided, however, that in each case, USAID or OIG determines that disclosure of the records to the DOJ is a use of the information that is compatible with the purpose for which the records were collected.

(b) Disclosure to any source from which additional information is requested in order to obtain information relevant to:

(1) A decision by either USAID or OIG concerning the hiring, assignment, or retention of an individual or other personnel action;

(2) The issuance, renewal, retention, or revocation of a security clearance;

(3) The execution of a security or suitability investigation;

(4) The letting of a contract; or

(5) The issuance, retention, or revocation of a license, grant, award, contract, or other benefit to the extent the information is relevant and necessary to a decision by USAID or OIG on the matter.

(c) Disclosure to a Federal, State, local, foreign, tribal, territorial, or other public authority in response to its request in connection with:

(1) The hiring, assignment, or retention, of an individual;

(2) The issuance, renewal, retention or revocation of a security clearance;

(3) The execution of a security or suitability investigation;

(4) The letting of a contract; or

(5) The issuance, retention, or revocation of a license, grant, award, contract, or other benefit conferred by that entity to the extent that the information is relevant and necessary to the requesting entity's decision on the matter.

(d) Disclosure in the event that a record, either by itself or in combination with other information, indicates a violation or a potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program stature, or by regulation, rule, or order issued pursuant thereto; or a violation or potential violation of a contract provision. In these circumstances, the relevant records in the system may be referred, as a routine use, to the appropriate entity, whether Federal, State, tribal, territorial, local or foreign, charged with the responsibility of investigating or prosecuting such

violation or charged with enforcing or implementing the statute, rule, regulation, order or contract.

(e) Disclosure to any source from which additional information is requested, either private or governmental, to the extent necessary to solicit information relevant to any investigation, audit, or evaluation.

(f) Disclosure to a foreign government pursuant to an international treaty, convention, or executive agreement entered into by the United States.

(g) Disclosure to contractors, grantees, consultants, or volunteers performing or working on a contract, service, grant, cooperative agreement, job or other activity for USAID or OIG, who have a need to access the information in the performance of their duties or activities. When appropriate, recipients will be required to comply with the requirements of the Privacy Act of 1974 as provided in 5 U.S.C. 552a(m).

(h) Disclosure to representatives of the Office of Personnel Management, the Office of Special Counsel, the Merit Systems Protection Board, the Federal Labor Relations Authority, the Equal Employment Opportunity Commission, the Office of Government Ethics, and other Federal agencies in connection with their efforts to carry out their responsibilities to conduct examinations, investigations, and/or settlement efforts, in connection with administrative grievances, complaints, claims, or appeals filed by an employee, and such other functions promulgated in 5 U.S.C. 1205-06.

(i) Disclosure to a grand jury agent pursuant to a Federal or State grand jury subpoena or to a prosecution request that such record be released for the purpose of its introduction to a grand jury.

(j) Disclosure in response to a facially valid subpoena for the record.

(k) Disclosure to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904, 2906.

(l) Disclosure to the Departments of the Treasury and Justice in circumstances in which OIG seeks to obtain, or has in fact obtained, and ex parte court order to obtain tax return information from the Internal Revenue Service.

(m) Disclosure to any Federal official charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures employed in investigative operations for purposed of reporting to the President and Congress on the activities of OIF as contemplated by the Homeland Security Act of 2002 (Pub. L. No. 107-296; November 25, 2002). This disclosure category includes other Federal offices of inspectors general and members of the President's Council on Integrity and Efficiency, and officials and administrative staff within their investigative chain of command, as well as authorized officials of DOJ and its component, the Federal Bureau of Investigation.

Disclosure to consumer reporting agencies: Not applicable.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: Paper records and all other media (photographs, audio recordings, diskettes, CD's etc) are stored in GSA-approved security containers with combination locks in a secured area. Electronic records are password protected and maintained on a file server in locked facilities that are secured at all times by security systems and video surveillance cameras.

Retrievability: Records are retrieved in a database by name and or alias, as well as by non-personally identifiable information, such as case number.

Safeguards: Access to paper records is restricted to authorized OIG employees on a need-to-know basis. At all times, paper records are maintained in locked safes in a secured area in offices that are occupied by authorized OIG employees. Access to electronic records is restricted to authorized OIG staff members on a need-to-know basis. Each person granted access to the system must be individually authorized to use the system. Disclosure of records maintained electronically is restricted through the use of passwords. The computer servers in which records are stored are password protected. Passwords are changed on a cyclical basis. The computer servers are located in locked facilities that are secured at all time by security systems and video surveillance cameras. The security systems provide immediate notification of any attempted intrusion to USAID Security personnel. All data exchanged between the servers and individual

computers is encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location.

Retention and disposal: Records relating to persons covered by this system are retained for two or five years after the investigation is closed. If an investigation does not involve allegations against a senior level USAID employee, is not of congressional interest, or does not yield a reportable result, the records within the closed case file are maintained for a period of two years from the date of closing by OIG. If the investigation yields a reportable result, has congressional interest, or involves allegations against a senior level USAID employee, the records within the closed case file will be retained for five years from the date of closing by OIG. After the applicable period (two or five years), closed investigative files will be sent from USAID, Office of Inspector General, 1300 Pennsylvania Ave, NW, Washington, DC, 20523, to the Washington National Records Center in Suitland, Maryland, where they will be retained for fifteen years, and subsequently destroyed. Any electronic file that qualifies as a record will be printed out and treated as a hard-copy record for disposition purposes.

Notification procedures: Records in this system are exempt from notification, access, and amendment procedure in accordance with subsections (j) and (k) of 5 U.S.C. 552a, and 22 CFR 215.13 and 215.14. Individuals requesting notification of the existence of records on themselves should send their request to the System Manager (see information above). The request must be in writing and include the requester's full name, his or her current address, his or her date and place of birth, and a return address for transmitting the information. The request shall be signed by either notarized signature or by signature

under penalty of perjury. Requesters shall also reasonably specify the record contents being sought.

Record access procedures: Individuals wishing to request access to a record on himself or herself must submit the request in writing according to the "Notification Procedures" above.

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 category: OIG collects information from a wide variety of sources, including information from USAID and other Federal, State and local agencies, subjects, witnesses, complainants, confidential and/or non-confidential sources, and other nongovernmental entities.

Exemptions claimed for the system: Under the specific authority provided by subsection (j)(2) of 5 U.S.C. 552a, USAID has adopted regulations, 22 CFR 215.13 and 215.14, which exempt this system from the notice, access, and amendment requirements of 5 U.S.C. 552a, except subsections (b); (c)(1) and (2); (e)(4)(A) through (F); (e)(6), (7), (9), (10), and (11); and (i). If the provision found at subsection (j)(2) of 5 U.S.C. 552a is held to be invalid, then, under subsections (k)(1) and (2) of 5 U.S.C. 552a, this system is determined to be exempt from the provisions of subsections (c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) of 5 U.S.C. 552a. See57 FR 38276, 38280-81 (August 24, 1992). The reasons for adoption of 22 CFR 215.13 and 215.14 are to protect the materials required by Executive order to be kept secret in the interest of national defense of foreign policy, to maintain the integrity of the law enforcement process, to ensure the proper functioning and integrity of law enforcement activities, to prevent disclosures of investigative techniques, to maintain the ability to obtain necessary information, to prevent subjects of investigation from frustrating the investigatory process, to avoid premature disclosure of the knowledge of criminal activity and the evidentiary basis of possible enforcement actions, to fulfill commitments made to sources to protect their identities and the confidentiality of information, and to avoid endangering these sources and law enforcement personnel.

Meredith Snee
Privacy Analyst

[FR Doc. 2013-09103 Filed 04/17/2013 at 8:45 am; Publication Date: 04/18/2013]