Vol 71, No. 207
October 26, 2006

Public Notice 5595
STATE–72
SYSTEM NAME:
Identity Management System (IDMS)
SECURITY CLASSIFICATION:
Sensitive But Unclassified
SYSTEM LOCATION:
Data covered by this system is maintained at the following locations: Department of State; 2201 C Street, NW.; Washington, DC 20520; domestic and overseas posts.
CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
The system will cover (1) Current and former Department of State, U.S. Agency for International Development (AID), and Peace Corps employees; (2) other individuals who require regular, ongoing access to agency facilities, including but not limited to certain applicants for employment or contracts; federal employees of other agencies; contractors; students; interns; volunteers; affiliates and other individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.), and (3) individuals formerly in any of these positions. The system does not apply to occasional visitors or short-term guests to whom the Department of State will issue temporary identification and credentials.
CATEGORIES OF RECORDS IN THE SYSTEM:
Records maintained on individuals issued identification by the Department of State include the following data fields: full name; Social Security number; date of birth; image (photograph); fingerprints; organization/ office of assignment; company name; telephone number; Personal Identity Verification (PIV) card issue and expiration dates; personal identification number (PIN); PIV request form; PIV registrar approval signature; PIV card number; emergency responder designation (if applicable); copies of documents used to verify identification or information derived from those documents such as document title, document issuing authority, document number, document expiration date and other document information; level of national security clearance and date granted; computer system user name; authentication certificates; digital signature information. Records maintained on card holders entering Department of State facilities or using Department of State systems include: Name; PIV Card number; date, time, and location of entry and exit; company name; level of national security clearance and expiration date; digital signature information; and computer networks/applications/data accessed.
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
5 U.S.C. 301; Federal Information Security Act (Pub. L. 104–106, sec. 5113); Electronic Government Act (Pub. L. 104–347, sec. 203); the Paperwork Reduction Act of 1995 (44 U.S.C. § 3501); and the Government Paperwork Elimination Act (Pub. L. 105–277, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; Federal Property and Administrative Act of 1949, as amended.
PURPOSE:
The primary purposes of the system are: (a) To ensure the safety and security

of Department of State facilities, systems, or information, and our occupants and users; (b) to verify that all persons entering federal facilities, using federal information resources, or accessing classified information are authorized to do so; (c) to track and control PIV cards issued to persons entering and exiting the facilities, using systems, or accessing classified information.

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

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 552a(b), and: (1) To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

(2) To notify another federal agency when, or verify whether, a PIV card is no longer valid.

(3) To the news media or the general public, factual information the disclosure of which would be in the public interest and which would not constitute an unwarranted invasion of personal privacy, consistent with Freedom of Information Act standards. Also see ''Routine Uses'' of Prefatory Statement published in the Federal Register.

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

STORAGE:

Records are stored in electronic media and in paper files.

RETRIEVABILITY:

Records are retrievable by name; Social Security number; other identification number; PIV card number; image (photograph) and fingerprint.

SAFEGUARDS:

Paper records are kept in locked cabinets in secure facilities and access to them is restricted to individuals whose role requires use of the records. The computer servers in which records are stored are located in facilities that are secured by alarm systems and offmaster key access. The computer servers themselves are password-protected. Access to individuals working at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the computer screen prior to display of records containing information about individuals. Data exchanged between the servers and the client at the guard stations and badging office are encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location. An audit trail is maintained and reviewed periodically to identify unauthorized access. Persons given roles in the PIV process must complete training specific to their roles to ensure they are knowledgeable about how to protect individually identifiable information.

RETENTION AND DISPOSAL:

Records relating to persons' access covered by this system are retained, retired and destroyed in accordance with Department of State Records Disposition Schedules approved by NARA. More information may be obtained by writing the Director; Office of Information Programs and Services; SA–2, Department of State; 515 22nd Street; Washington, DC; 20522–8100. In accordance with HSPD–12, Department of State Identification Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. Department of State Identification Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

SYSTEM MANAGER(S) AND ADDRESS:
Director; Domestic Facility Protection; Bureau of Diplomatic Security; Department of State; 2201 C Street, NW., 20522.

NOTIFICATION PROCEDURES:
An individual can determine if this system contains a record pertaining to him/her by sending an originally signed request in writing, to the Director; Office of Information Programs and Services (address above). The individual must specify that he or she wants the Bureau of Diplomatic Security's Identity Management System to be checked. When requesting notification of or access to records covered by this Notice, an individual should provide his/her full name, date and place of birth, current mailing address and zip code, signature, brief description of the circumstances which may have caused the creation of the record, agency name, and work location in order to establish identity.

RECORDS ACCESS ROCEDURES:
Same as notification procedures. Requesters should also reasonably specify the record contents being sought. Rules regarding access to Privacy Act records appear in 22 CFR part 171. If additional information or assistance is required, contact the Director (address above).

CONTESTING RECORD PROCEDURES:
Same as notification procedures. Requesters should also reasonably identify the record, specify the information they are contesting, state the corrective action sought and the reasons for the correction along with supporting justification showing why the record is not accurate, timely, relevant, or complete. Rules regarding amendment of Privacy Act records appear in 22 CFR part 171. If additional information or assistance is required, contact the Director; Office of Information Programs and Services (address above).

RECORD SOURCE CATEGORIES:
Employee, contractor, or applicant; sponsoring agency; former sponsoring agency; other federal agencies; contract employer; and former employer.

EXEMPTIONS CLAIMED FOR THE SYSTEM:
None.