

Volume 75, Number 166

August 27, 2010

Public Notice 7132

STATE-07

SYSTEM NAME:

Cryptographic Clearance Records.

SYSTEM CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Department of State, 301 4th St., SW.,
Room 750 Washington, DC

20547.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All current Civil Service and Foreign Service direct hire employees of the Department of State and Agency for International Development who have applied for cryptographic clearances as well as those who have already received cryptographic clearance.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains employee name; the position held by an employee; correspondence from the Bureau of Diplomatic Security concerning an individual's clearance; and the date the clearance was granted or denied.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Executive Order 13526.

PURPOSE:

The information contained in these records is used to protect the Bureau of Information Resource Management's cryptographic duties and to protect sensitive information from unauthorized disclosure. Information relating to an employee's eligibility for cryptographic clearance is used solely by the Bureau of Information Resource Management.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF

USERS AND THE PURPOSES OF SUCH USES:

The Department of State periodically publishes in the Federal Register its standard routine uses that apply to all of its Privacy Act systems of records. These notices appear in the form of a Prefatory Statement. These standard routine uses apply to the Cryptographic Clearance Records, State-07.

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

STORAGE:

Hard copy; magnetic computer media.

RETRIEVABILITY:

By individual name.

SAFEGUARDS:

All users are given information system security awareness training, including the procedures for handling Sensitive but Unclassified information and personally identifiable information. Annual refresher training is mandatory. Before being granted access to Cryptographic Clearance Records, a user must first be granted access to the Department of State computer system.

All Department of State employees and contractors with authorized access have undergone a thorough background security investigation.

Access to the Department of State, its annexes and posts abroad is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All paper records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel only.

Access to computerized files is

password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage. When it is determined that a user no longer needs access, the user account is disabled.

RETENTION AND DISPOSAL:

Records are retired in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA). More specific information may be obtained by writing the Director, Office of Information Programs and Services, Department of State, SA-2, 515 22nd Street, NW., Washington, DC 20522-8001.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Cryptographic Services Branch, Systems Integrity Division, Bureau of Information Resource Management, Room 750, SA-44, 301 4th Street, SW., Washington, DC 20547.

NOTIFICATION PROCEDURE:

Individuals who have cause to believe that the Cryptographic Services Branch might have records pertaining to them should write to the Director, Office of Information Programs and Services, Department of State, SA-2, 515 22nd Street, NW., Washington, DC 20522-8001. The individual must specify that he/she wishes the records of the Systems Integrity Division to be checked. At a minimum, the individual must include: Name; date and place of birth; current mailing address and zip code; signature; the approximate dates of employment with the Department of State; and the nature of such employment.

RECORD ACCESS PROCEDURES:

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services (address above).

CONTESTING RECORD

PROCEDURES:

(See above).

RECORD SOURCE CATEGORIES:

The individual; Cryptographic Services Branch.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.