being considered for detail, assignment or secondment.

(5) Officials of foreign governments and other U.S. Government agencies for clearance before a Federal employee is assigned to that country as well as for the procurement of necessary services for American personnel assigned overseas, such as permits of free entry and identity cards;

(6) Attorneys, union representatives or other persons designated in writing by employees who are the subject of the information to represent them in complaints, grievances, or other litigation.

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 Office of the Coordinator for Reconstruction and Stabilization Records, State–68.

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

STORAGE:

Electronic media.

RETRIEVABILITY:

Individual's name or system generated identification number.

SAFEGUARDS:

The Department of State will maintain responsibility for keeping the records accurate and updated; however, a limited number of U.S. Agency for International Development (USAID) personnel will be allowed to access the CRC database in order to run the Civilian Deployment Center. These USAID personnel will use a State Department-approved remote access program in order to enter the State system. All Department of State and USAID employees and contractors with authorized access have undergone a thorough background security investigation. All users must take mandatory annual cyber security awareness training including the procedures for handling Sensitive But Unclassified and personally identifiable information. Before being granted access to the Office of the Coordinator for Reconstruction and Stabilization Records, a user must first be granted access to Department of State computer systems.

Remote access to the Department of State network from non-Department owned systems is only authorized through a Department-approved remote access program. Remote access to the network is configured with two factor authentication and time-out functions.

Access to the Department and its annexes is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Servers are stored in Department of State secured facilities in cipher locked server rooms. Access to electronic 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:

These records will be maintained with published record disposition schedules of the Department of State as approved by the National Archives and Records Administration (NARA). More specific information may be obtained by writing to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, 515 22nd Street, NW., Washington, DC 20522–8100.

SYSTEM MANAGER AND ADDRESS:

Office of the Coordinator for Reconstruction and Stabilization, Department of State, SA–3, 2121 Virginia Avenue, NW., Washington, DC 20520.

NOTIFICATION PROCEDURE:

Individuals who have reason to believe that the Office of the Coordinator for Reconstruction and Stabilization might have records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, 515 22nd Street, NW., Washington, DC 20522–8100. The individual must specify that he or she wishes the records of the Office of the Coordinator for Reconstruction and Stabilization to be checked. At a minimum, the individual should include: Name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Office of the Coordinator for Reconstruction and Stabilization has records pertaining to them.

RECORD ACCESS AND AMENDMENT 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:

These records contain information that is obtained from the individual who is the subject of the records.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

[FR Doc. 2010–21432 Filed 8–26–10; 8:45 am]

BILLING CODE 4710–24–P

DEPARTMENT OF STATE

[Public Notice 7132]

State–07, Cryptographic Clearance Records

Summary: Notice is hereby given that the Department of State proposes to amend an existing system of records, Cryptographic Clearance Records, State-07, pursuant to the provisions of the Privacy Act of 1974, as amended (5 U.S.C. 552a) and Office of Management and Budget Circular No. A–130, Appendix I. The Department's report was filed with the Office of Management and Budget on July 27, 2010.

It is proposed that the current system will retain the name "Cryptographic Clearance Records." It is also proposed that the amended system description will include revisions/additions to the: Categories of individuals, Categories of records, Authority for maintenance of the system, Purpose, Safeguards and Retrievability as well as other administrative updates.

Any persons interested in commenting on the amended system of records may do so by submitting comments in writing to Margaret P. Grafeld, Director, Office of Information Programs and Services, A/GIS/IPS, Department of State, SA–2, 515 22nd Street, NW., Washington, DC 20522–8001. This system of records will be effective 40 days from the date of publication, unless we receive comments that will result in a contrary determination.

The amended system description, "Cryptographic Clearance Records, State–07," will read as set forth below.

Dated: July 27, 2010.

Steven J. Rodriguez,

Deputy Assistant Secretary of Operations, Bureau of Administration, U.S. Department of State.

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.

[FR Doc. 2010–21429 Filed 8–26–10; 8:45 am]

BILLING CODE 4710–24–P

SUSQUEHANNA RIVER BASIN COMMISSION

Notice of Public Hearing and Commission Meeting

AGENCY: Susquehanna River Basin Commission.

ACTION: Notice of public hearing and Commission meeting.

SUMMARY: The Susquehanna River Basin Commission will hold a public hearing as part of its regular business meeting on September 16, 2010, in Corning, NY. At the public hearing, the Commission will consider: (1) Action on certain water resources projects; (2) compliance matters involving three projects; (3) action on a project involving a diversion; and (4) the rescission of two docket approvals. Details concerning the matters to be addressed at the public hearing and business meeting are contained in the **SUPPLEMENTARY INFORMATION** section of this notice.

DATES: September 16, 2010, at 8:30 a.m.

ADDRESSES: Radisson Hotel Corning, 125 Denison Parkway East, Corning, NY 14830.

FOR FURTHER INFORMATION CONTACT: Richard A. Cairo, General Counsel, *telephone:* (717) 238–0423, ext. 306; *fax:* (717) 238–2436; *e-mail: rcairo@srbc.net* or Stephanie L. Richardson, Secretary to the Commission, *telephone:* (717) 238–0423, ext. 304; *fax:* (717) 238–2436; *e-mail: srichardson@srbc.net.*

SUPPLEMENTARY INFORMATION: In addition to the public hearing and its related action items identified below,