Department of State

[Public Notice: 12013]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: The information collected and maintained in the Cryptographic Clearance Records system is used by the Bureau of Information Resource Management in the Department of State to determine an employee's eligibility for cryptographic clearance and to protect cryptographic duties and sensitive information from unauthorized disclosure.

DATES: In accordance with 5 U.S.C. § 552a(e)(4) and (11), this system of records notice is effective upon publication, with the exception of the routine uses (a) and (b) that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by [*INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER*].

ADDRESSES: Questions can be submitted by mail, email, or by calling Eric F. Stein, the Senior Agency Official for Privacy on (202) 485-2051. If mail, please write to: U.S Department of State; Office of Global Information Systems, A/GIS; Room 4534, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, Eric F. Stein, at Privacy@state.gov. Please write "Cryptographic Clearance Records, State-07" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS; Room

4534, 2201 C St., N.W.; Washington, DC 20520 or by calling (202) 485-2051.

SUPPLEMENTARY INFORMATION: The purpose of this modification is to make substantive and administrative changes to the previously published notice. This notice modifies the following sections: Summary, Dates, Addresses, For Further Information Contact, Supplementary Information, System Location(s), Categories of Records in the System, Policies and Procedures for Retrieval of Records, Routine Uses of Records Maintained in the System, Policies and Practices for Storage of Records, Policies and Practices for Retention and Disposal of Records, and Administrative, Technical, and Physical Safeguards. In addition, this notice makes administrative updates to the following sections: Record Access Procedures, Notification Procedures, and History. This notice is being modified to reflect new OMB guidance, new routine uses and categories of records, updated contact information, and a notice publication history.

SYSTEM NAME AND NUMBER: Cryptographic Clearance Records, State-07.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION(S): Department of State, ESOC West, Building 17, 1 Denver Federal Center, Denver, Colorado 80225.

SYSTEM MANAGER(S): Chief, Cryptographic Services Branch, Systems Integrity Division, Bureau of Information Resource Management, SA-07B, 7958 Angus Ct, Springfield, VA 22153. The system manager can be reached on cryptoaccesspgm@state.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

- 22 U.S.C. § 4802 (Diplomatic Security) (Responsibility of Secretary of State);
- 5 U.S.C. § 301 (Management of Executive Agencies);
- 5 U.S.C. Chapter 73 (Suitability, Security, and Conduct);

- Executive Order 13526 (Classified National Security Information)***;***
- CNSS Policy No. 3, dated October 2007 (National Policy on Granting Access to U.S. Classified Cryptographic Information);
- Executive Order 12968, as amended (Access to Classified Information);
- Executive Order 13467, as amended (Reforming Processes Related to Suitability for Government Employment, Fitness, for Contractor Employees, and Eligibility for Access to Classified National Security Information); and
- Security Executive Agent Directive 4 (National Security Adjudicative Guidelines).

PURPOSE(S) OF THE SYSTEM: The information collected and maintained in the Cryptographic Clearance Records system is used by the Bureau of Information Resource Management in the Department of State to determine an employee's eligibility for cryptographic clearance and to protect cryptographic duties and sensitive information from unauthorized disclosure.

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. The Privacy Act defines an individual at 5 U.S.C. § 552a (a)(2) as a United States citizen or lawful permanent resident.

CATEGORIES OF RECORDS IN THE SYSTEM: This system contains employee name, last four digits of social security number (SSN), date of birth (DOB), Foreign Service (FS) HR ID number, FS skill code, position held by an employee, correspondence from the Bureau of Diplomatic Security concerning an individual's clearance, and date the clearance was granted or denied.

RECORD SOURCE CATEGORIES: These records contain information obtained from the individual who is the subject of these records and Cryptographic Services Branch personnel.

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

The information in Cryptographic Clearance Records system may be disclosed to the following:

(a.) Appropriate agencies, entities, and persons when (1) the Department of State suspects or has confirmed that there has been a breach of the system of records; (2) the Department of State has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of State (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of State efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(b.) Another Federal agency or Federal entity, when the Department of State determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

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 (published in Volume 73, Number 136, Public Notice 6290, on July 8 15, 2008). All these standard routine uses apply to Cryptographic Clearance Records, State-07.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored in hard copy and magnetic computer media. A description of standard Department of State policies concerning storage of electronic records is found here https://fam.state.gov/FAM/05FAM/05FAM0440.html.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by individual name, last four digits of SSN, DOB, and Foreign Service (FS) HR ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retired and destroyed in accordance with published Department of State Records Disposition Schedules as approved by the National Archives and Records Administration (NARA) and outlined here https://foia.state.gov/Learn/RecordsDisposition.aspx. The retention period for records maintained in the system is twenty years. More specific information may be obtained by writing to the following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All users are given cyber security awareness training which covers the procedures for handling Sensitive but Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Department OpenNet users are required to take the Foreign Service Institute distance learning course instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly. 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 to records maintained in this system of records 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. 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.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or amend records pertaining to themselves should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Cryptographic Clearance Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; 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 Cryptographic Clearance Records include records pertaining to him or her. Detailed instructions on Department of State procedures for accessing and amending records can be found on the Department's FOIA website at https://foia.state.gov/Request/Guide.aspx.

CONTESTING RECORD PROCEDURES: Individuals who wish to contest record procedures should write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to them may write to U.S. Department of State; Director, Office of Information Programs and Services**;** A/GIS/IPS; 2201 C Street, N.W., Room B-266; Washington, DC 20520. The individual must specify that he/she wishes the Cryptographic Clearance Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; current mailing address and zip code; date and place of birth; notarized signature or statement under penalty of perjury; 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 Cryptographic Clearance Records system include records pertaining to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Previously published in the *Federal Register* on August 27, 2010 in Volume 75, Number 166, Public Notice 7132.

Eric F. Stein,

Deputy Assistant Secretary,

Global Information Services (A/GIS),

U.S. Department of State.

Billing Code: 4710-AD