[Billing Code: 4710-43]

DEPARTMENT OF STATE

[Public Notice: 9381]

Privacy Act; System of Records: Security Records, State-36.

SUMMARY: Notice is hereby given that the Department of State proposes to amend an existing system of records, Security Records, State-36, 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.

DATES: This system of records will be effective on [INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless we receive comments that will result in a contrary determination.

ADDRESSES: Any persons interested in commenting on the amended system of records may do so by writing to the Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW; Washington, DC 20522-8100.

FOR FURTHER INFORMATION CONTACT: John Hackett, Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street NW; Washington, DC 20522-8100, or at Privacy@state.gov.

SUPPLEMENTARY INFORMATION: The Department of State proposes that the current system will retain the name "Security Records" (previously published at 78 FR 27276, May 9, 2013). The records maintained in State-36, Security Records, capture data related to incidents and threats affecting U.S. Government personnel, U.S. Government information, or U.S. Government facilities world-wide, for a variety of legal purposes including federal and state law enforcement and counterterrorism purposes. The information maintained in Security Records may be used to determine general suitability for employment or retention in employment, to grant a contract or issue a license, grant, or security clearance. The proposed system will include modifications and administrative updates to the following sections: Categories of individuals and Categories of records. Additionally, records regarding the Office of Foreign Missions were removed and included in a new SORN to provide greater transparency of their records.

The Department's report was filed with the Office of Management and Budget. The amended system description, "Security Records, State-36," will read as set forth below.

_____

Joyce A. Barr,
Assistant Secretary for Administration,

U.S. Department of State

STATE-36

SYSTEM NAME:

Security Records.

SECURITY CLASSIFICATION:

Unclassified and Classified.

SYSTEM LOCATION:

Department of State and its annexes, Bureau of Diplomatic Security, and various field and regional offices throughout the United States, and abroad at some U.S. Embassies, U.S. Consulates General, and U.S. Consulates.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Present and former employees of the Department of State; applicants for Department employment who are presently being investigated for security clearance; contractors working for the Department; interns and detailees to the Department; employees of other federal agencies who have accounts on our Department networks; individuals requiring access to the official Department of State premises who have undergone or are undergoing security clearance; some passport and visa applicants concerning matters of adjudication; individuals and institutions identified in passport and visa crime investigations; individuals involved in

unauthorized access to classified information; prospective alien spouses of U.S. citizen employees of the Department of State; individuals or groups whose activities have a potential bearing on the security of Departmental or Foreign Service operations, domestically or abroad, including those involved in criminal or terrorist activity; individuals and organizations who apply to be constituents in the exchange of security information from public-private partnerships; and visitors to the Department of State main building (Harry S Truman Building), to its domestic annexes, field offices, missions, and to the U.S. Embassies and U.S. Consulates and missions overseas. Also covered are individuals issued security or cybersecurity violations or infractions; litigants in civil suits and criminal prosecutions of interest to the Bureau of Diplomatic Security; individuals who have Department building passes; individuals using Department devices or networks; uniformed security officers; individuals named in congressional inquiries to the Bureau of Diplomatic Security; individuals subject to investigations conducted abroad on behalf of other federal agencies; and individuals whose activities other agencies believe may have a bearing on U.S. foreign policy interests.

CATEGORIES OF RECORDS IN THE SYSTEM:

Incident and investigative material relating to any category of individual described above, including case files containing items such as name, date and place of birth, citizenship, telephone numbers, addresses, physical description (including height, weight, body type, hair, clothing, gender, ethnicity, race, and other general and distinguishing physical features), accent description, identification media (such as passport, residency, or driver's license numbers), vehicle registration and vehicle information; email address, family identifiers (such as names of relatives and biographic information), employer identifiers, applications for passports and employment, photographs, biometric data (to include fingerprints, and deoxyribonucleic acid (DNA) information), birth certificates, credit checks, security evaluations and clearances, other agency reports and informant reports; legal case pleadings and files; evidence collected during investigations; polygraphs; network audit records, network use records, email, chat conversations, and text messages sent using Department devices or networks; social media account findings for individuals undergoing security investigations; security violation files; training reports; weapons assignment database; firing proficiency and other security-related testing scores; availability for special protective assignments; language proficiency

scores; intelligence reports; counterintelligence material; counterterrorism material; internal Departmental memoranda; internal personnel, fiscal, and other administrative documents; emergency contact information for Department employees and contractors; Social Security number; specific areas and times of authorized accessibility; escort authority; status and level of security clearance; issuing agency and issue date; and for all individuals: date and times of building entrance and exit.

For visitors, information collected can include name, date of birth, citizenship, identification type, identification number, temporary badge number, host's name, office symbol, room number, and telephone number. For public-private partnerships to exchange security information, information collected can include name, address, telephone number and email address.

Security files contain information needed to provide protective services for the Secretary of State and visiting and resident foreign officials and associated foreign official facilities, and to protect the Department's official facilities and information assets. Security files contain documents and reports furnished to the Department by other agencies concerning individuals whose activities the other agencies believe may have a bearing on U.S. foreign policy interests.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

(a) 5 U.S.C. 301 (Government Organization and Employees) (Departmental regulations); (b) 5 U.S.C. Chapter 73 (Suitability, Security, and Conduct); (c) 5 U.S.C. 7531-33 (National Security); (d) 8 U.S.C. 1104 (Enforcement of immigration and nationality laws); (e) 18 U.S.C. 111 (Crimes and Criminal Procedures) (Assaulting, resisting, or impeding certain officers or employees); (f) 18 U.S.C. 112 (Protection of foreign officials, official guests, and internationally protected persons); (g) 18 U.S.C. 201 (Bribery of public officials and witnesses); (h) 18 U.S.C.1030 (Fraud and related activity in connection with computers); (i) 18 U.S.C. 1114 (Protection of officers and employees of the U.S.); (j) 18 U.S.C. 1116 (Murder or manslaughter of foreign officials, official guests, or internationally protected persons); (k) 18 U.S.C. 1117 (Conspiracy to murder); (l) 18 U.S.C. 1541-1546 (Issuance without authority, false statement in application and use of passport, forgery or false use of passport, misuse of passport, safe conduct violation, fraud and misuse of visas, permits, and other documents); (m) 22 U.S.C. 211a (Foreign Relations and Intercourse) (Authority to grant, issue, and verify passports); (n) 22 U.S.C. 842, 846, 911 (Duties of Officers and Employees and Foreign Service Officers) (Repealed, but applicable to past records); (o) 22

U.S.C. 2454 (Administration); (p) 22 U.S.C. 2651a (Organization of the Department of State); (q) 22 U.S.C. 2658 (Rules and regulations; promulgation by Secretary; delegation of authority) (Repealed, but applicable to past records); (r) 22 U.S.C. 2709 (Special Agents); (s) 22 U.S.C. 2712 (Authority to control certain terrorism-related services); (t) 22 U.S.C. 3921 (Management of the Foreign Service); (u) 22 U.S.C. 4802 (Diplomatic Security) (Responsibility of Secretary of State), (v) 22 U.S.C.4804(3)(D) (Responsibilities of Assistant Secretary for Diplomatic Security) (Repealed, but applicable to past records); (w) 22 U.S.C. 4831-4835 (Accountability review, accountability review board, procedures, findings and recommendations by a board, relation to other proceedings); (x) 44 U.S.C. 31 (Federal Records Act of 1950, Sec. 506(a), as amended) (applicable to past records); (y) 44 U.S.C. 3541 (Federal Information Security Management); (z) Executive Order 10450 (Security requirements for government employment); (aa) Executive Order 12107 (Relating to the Civil Service Commission and Labor-Management in the Federal Service); (bb) Executive Order 13526 and its predecessor orders (National Security Information); (cc) Executive Order 12968 (Access to Classified Information); (dd) Executive Order 13587 (Security of Classified Networks and Information); (ee) Executive Order 13470 and its predecessor orders

(United States Intelligence Activities); (ff) 22 CFR Subchapter M (International Traffic in Arms) (applicable to past records); (gg) 40 U.S.C. Chapter 10 (Federal Property and Administrative Services Act (1949)); (hh) 31 U.S.C. (Internal Revenue Code); (ii) Pub. L. 99-399, 8/27/1986 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended); (jj) Pub. L. 100-202, 12/22/1987 (Appropriations for Departments of Commerce, Justice, and State) (applicable to past records); (kk) Pub. L. 100-461, 10/1/1988 (Foreign Operations, Export Financing, and Related Programs Appropriations Act); (ll) Pub. L. 107-56, 10/26/2001 (USA PATRIOT Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); (mm) Pub. L.108-21, 4/30/2003 (PROTECT Act - Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003); (nn) Executive Order 12356 (National Security Information) (applicable to past records); (oo) Executive Order 9397 (Numbering System for Federal Accounts Relating to Individual Persons); (pp) HSPD-12, 8/27/2004 (Homeland Security Presidential Directive); (qq) Executive Order 13356, 8/27/2004 (Strengthening the Sharing of Terrorism Information to Protect Americans); (rr) Pub. L. 108-458 (Section 1016), 12/17/2004 (Intelligence

Reform and Terrorism Prevention Act of 2004; (ss) Pub. L. 92-463: 5 U.S.C. App. (Federal Advisory Committee Act).

PURPOSE(S):

The records maintained in State-36, Security Records, capture data related to incidents and threats affecting U.S. Government personnel, U.S. Government information, or U.S. Government facilities world-wide, for a variety of legal purposes including federal and state law enforcement and counterterrorism purposes. The information maintained in Security Records may be used to determine general suitability for employment or retention in employment, to grant a contract or issue a license, grant, or security clearance.

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

The information in Security Records is used by:

(a) Department of State officials in the administration of their responsibilities;

(b) Appropriate committees of Congress in furtherance of their respective oversight functions;

(c) Department of Treasury; U.S. Office of Personnel Management; Agency for International Development; Department of Commerce; Peace Corps; Department of Defense; Central Intelligence Agency; Department of Justice; Department of Homeland Security; National Counter Terrorism Center; and other federal agencies inquiring pursuant to law or Executive Order, in order to make a determination of general suitability for employment or retention in employment, to grant a contract or issue a license, grant, or security clearance;

(d) Any federal, state, municipal, foreign or international law enforcement or other relevant agency or organization as needed for security, law enforcement or counterterrorism purposes, such as: threat alerts and analyses, protective intelligence and counterintelligence information, information relevant for screening purposes;

(e) Any other agency or department of the federal government pursuant to statutory intelligence responsibilities or other lawful purposes;

(f) Any other agency or department of the Executive Branch having oversight or review authority with regard to its investigative responsibilities;

(g) A federal, state, local, foreign, or international agency or other public authority that investigates, prosecutes, or assists in investigation or prosecution of violation of criminal law or enforces, implements, or assists in enforcement or implementation of statute, rule, regulation, or order;

(h) A federal, state, local or foreign agency or other public authority or professional organization maintaining civil, criminal, and other relevant enforcement or pertinent records such as current licenses; information may be given to a consumer reporting agency:

(1) to obtain information, relevant enforcement records or other pertinent records such as current licenses, or

(2) to obtain information relevant to an agency investigation, a decision concerning the hiring or retention of an employee or other personnel action, the issuance of a security clearance or the initiation of administrative, civil, or criminal action;

(i) Officials of government agencies in the letting of a contract, issuance of a license, grant or other benefit, and the establishment of a claim;

(j) Any private or public source, witness, or subject from which information is requested in the course of a legitimate agency investigation or other inquiry, to the extent necessary to identify an individual; to inform a source, witness or subject of the nature and purpose of the investigation or other inquiry; and to identify the information requested;

(k) An attorney or other designated representative of any source, witness or subject described in paragraph (j) of the Privacy Act only to the extent that the information would be provided to that category of individual itself in the course of an investigation or other inquiry;

(l) A federal agency following a response to its subpoena or to a prosecution request that such record be released for the purpose of its introduction to a grand jury or other criminal proceeding;

(m) Relevant information may be disclosed from this system to the news media and general public in furtherance of a legitimate law enforcement or public safety function as determined by the

Department, e.g., to assist in the location of federal fugitives, to provide notification of arrests, to provide alerts, assessments, or similar information on potential threats to life, health, or property, or to keep the public appropriately informed of other law enforcement or Department matters or other matters of legitimate public interest where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy and could not reasonably be expected to prejudice the outcome of a pending or future trial;

(n) State, local, federal or non-governmental agencies and entities as needed for purposes of emergency or disaster response; and

(o) U.S. government agencies within the framework of the National Suspicious Activity Report (SAR) Initiative (NSI) regarding foreign intelligence and terrorist threats, managed by the Department of Justice.

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 Security Records, State-36.

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

STORAGE:

Physical and electronic media.

RETRIEVABILITY:

By individual name, personal or biometric identifier, case number, badge number, and Social Security number (for other than visitors), as well as by each category of records in the system.

SAFEGUARDS:

All users are given cybersecurity awareness training which covers the procedures for handling Sensitive But Unclassified information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Foreign Service and Civil Service employees and those Locally Engaged Staff who handle PII are required to take the FSI 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 Security Records, a user must first be granted access to the

Department of State computer system, and user access is not granted until a background investigation has been completed.

Remote access to the Department of State network from non-Department owned systems is authorized only through a Department-approved access program. Remote access to the network is configured with the Office of Management and Budget Memorandum M-07-16 security requirements, which include but are not limited to two-factor authentication and time out function.

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. 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:

Retention of these records varies depending upon the specific kind of record involved. The records are retired or destroyed in accordance with published schedules of the Department of State and as approved by the National Archives and Records Administration. 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:

Principal Deputy Assistant Secretary for Diplomatic Security and Director for the Diplomatic Security Service; Department of State; SA-20; 23rd Floor; 1801 North Lynn Street; Washington, DC 20522-2008 for the Harry S Truman Building, domestic annexes, field offices and missions; Security Officers at respective U.S. Embassies, Consulates, and missions overseas.

NOTIFICATION PROCEDURE:

Individuals who have reason to believe that the Bureau of Diplomatic Security may have security/investigative records pertaining to themselves 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/she wishes Security Records to be checked. At a minimum, the individual must include: name; date and place of birth; current mailing address and zip code; signature; and a brief description of the circumstances which may have caused the creation of the record.

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 obtained from the individual; persons having knowledge of the individual; persons having knowledge of incidents or other matters of investigative interest to the Department; other U.S. law enforcement agencies and court systems; pertinent records of other federal, state, or local agencies or foreign governments; pertinent records of private firms or organizations; the intelligence community; and other public sources. The records also contain information obtained from

interviews, review of records, and other authorized investigative techniques.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Any other exempt records from other agencies' systems of records that are recompiled into this system are also considered exempt to the extent they are claimed as such in the original systems.

Pursuant to 5 U.S.C. 552a (j)(2), records in this system may be exempted from subsections (c)(3) and (4), (d), (e)(1), (2), (3), and (e)(4)(G), (H), and (I), and (f) of the Privacy Act. Pursuant to 5 U.S.C. 552a (k)(1), (k)(2), and (k)(5), records in this system may be exempted from subsections (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (d)(5), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), (f)(1), (f)(2), (f)(3), (f)(4), and (f)(5).

See 22 CFR 171.

[FR Doc. 2015-31527 Filed: 12/14/2015 8:45 am; Publication Date: 12/15/2015]