Billing Code: 4710-24

DEPARTMENT OF STATE

[Public Notice 10450]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: This system of records, Security Records, captures 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, counterterrorism purposes, and administrative security functions.

DATES: This system of records notice is effective upon publication, with the exception of the new or modified routine uses (b), (c), (d), (e), (m), (n), (p), (q), (r), (s), (t), and (u) 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 or email. If mail, please write to: U.S Department of State; Office of Global Information Systems, Privacy Staff ; A/GIS/PRV; SA–2, Suite 8100; Washington, DC 20522-0208. If email, please address the email to the Senior Agency Official for Privacy, Mary R. Avery, at

Privacy@state.gov or call (202) 663-2215. Please write "Security Records, State-36" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Mary R. Avery, Senior Agency Official for Privacy; U.S. Department of State; Office of Global Information Services, A/GIS/PRV; SA–2, Suite 8100; Washington, DC 20522-0208; at Privacy@state.gov, or (202) 663-2215 .

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, the Department of State proposes to consolidate two record systems: Security Records, State-36 (previously published at 80 FR 77691) and Identity Management System, State-72 (previously published at 71 FR 62653) under Security Records, State-36. These two systems are being merged because the records and system purposes are substantially related. This notice modifies the following sections of State-36, Security Records: System Location; Authority for Maintenance of the System; Purposes of the System; Categories of Individuals Covered by the System; Categories of Records in the System; Routine Uses of Records Maintained in the System, including categories of users and purposes of such uses; 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: Policies and Procedures for Retrieval of Records, Record Access Procedures, Notification Procedures, and History. These changes reflect the incorporation of State-72 into State-36, the Department's move to cloud storage, new OMB guidance, expanded authorities and routine uses for these records, updated contact information, and a

notice publication history.

SYSTEM NAME AND NUMBER: State-36, Security Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Department of State, located at 2201 C Street NW, Washington, DC 20520, 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. Within a government certified cloud provided, implemented, and overseen by the Department's Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington DC 20520.

SYSTEM MANAGER(S): 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. The Principal Deputy Assistant Secretary for Diplomatic Security can be reached at (571) 345-3815.

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 USC 2708 (Department of State Rewards Program); (s) 22 U.S.C. 2709 (Special Agents); (t) 22 U.S.C. 2712 (Authority to control certain terrorism-related services); (u) 22 U.S.C. 3921 (Administration by Secretary of State); (v) 22 U.S.C. 4802 (Diplomatic Security) (Responsibility of Secretary of State), (w) 22 U.S.C.4804(3)(D) (Responsibilities of Assistant Secretary for Diplomatic Security) (Repealed, but applicable to past records); (x) 22 U.S.C. 4831-4835 (Accountability review, accountability review board, procedures, findings and recommendations by a board, relation to other proceedings); (y) 22 U.S.C. Sec. 4807 (Establishment of Visa and Passport Security Program in the Department of State) (z) 44 U.S.C. 31 (Federal Records Act of 1950, Sec. 506(a), as amended) (applicable to past records); (aa) 44 U.S.C. 3541 (Federal Information Security Management); (bb) Executive Order 10450 (Security requirements for

government employment)(revoked but applicable to past records) and its successor orders; (cc) Executive Order 12107 (Relating to the Civil Service Commission and Labor-Management in the Federal Service); (dd) Executive Order 13526 and its predecessor orders (Classified National Security Information); (ee) Executive Order 12968, as amended (Access to Classified Information); (ff) Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and Information); (gg) Executive Order 12333, as amended, and its predecessor orders (United States Intelligence Activities); (hh) 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); (ii) 22 CFR Subchapter M (International Traffic in Arms) (applicable to past records); (jj) 40 U.S.C. Chapter 10 (Federal Property and Administrative Services Act (1949)); (kk) 31 U.S.C. (Internal Revenue Code); (ll) Pub. L. 99-399, 8/27/1986 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended); (mm) Pub. L. 100-202, 12/22/1987 (Appropriations for Departments of Commerce, Justice, and State) (applicable to past records); (nn) Pub. L. 100-461, 10/1/1988 (Foreign Operations, Export Financing, and Related Programs Appropriations Act); (oo) Pub. L. 104-347, sec. 203 (Electronic Government Act); (pp) Pub. L. 107-56, 10/26/2001 (USA PATRIOT Act - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); (qq) Pub. L.108-21, 4/30/2003 (PROTECT Act - Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003); (rr) Executive Order 12356 (National Security Information) (applicable to past records); (ss) Executive Order 9397 (Numbering System for Federal Accounts Relating to

Individual Persons); (tt) Homeland Security Presidential Directive (HSPD-12) (Policy for a Common Identification Standard for Federal Employees and Contractors, 8/27/2004; (uu) Executive Order 13356 (Strengthening the Sharing of Terrorism Information to Protect Americans); (vv) P.L. 108-458 (Sect.1016), 12/17/2004 (Intelligence Reform and Terrorism Prevention Act of 2004; (ww) P.L. 92-463: 5 U.S.C. App. (Federal Advisory Committee Act); (xx) E.O. 12829, National Industrial Security Program; (yy) PDD/NSC-12 Security Awareness and Reporting Foreign Contacts; (yy) Security Executive Agent Directive 3 (Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position); (zz) Security Executive Agent Directive 4 (National Security Adjudicative Guidelines); (aaa) Security Executive Agent Directive 5 (Social Media in Background Investigations).

PURPOSE(S) OF THE SYSTEM: 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, state, and international 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, national security eligibility, security clearance, or Department credential (including PIV card).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Present and former employees of the Department of State; U.S. Agency for International Development (AID), and Peace Corps employees; applicants for Department

employment who are presently undergoing a background investigation; individuals communicating on publicly available social media with employees or applicants undergoing a background investigation; contractors working for the Department; interns and detailees to the Department; employees of other federal agencies who have accounts on 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 and institutions identified in investigations regarding identity theft or document fraud affecting or relating to the programs, functions or authorities of the Department of State; individuals identified in investigations of Federal offenses committed within the special maritime and territorial jurisdiction of the United States; 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; individuals who participate in Department rewards programs; and individuals whose activities other agencies believe may have a bearing on U.S. foreign policy interests. 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: 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), medical records, 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, national security eligibility determinations, fitness determinations, 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 communications and/or findings for individuals undergoing background or security investigations; publicly available social media communications of third parties with individuals undergoing background

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; threat information pertaining to private U.S. entities and individuals operating overseas;
internal Departmental memoranda; internal personnel, fiscal, and other administrative documents, to include PIV-related 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.

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.

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 and subcommittees 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 or verify general suitability for employment, fitness, or retention in employment, to grant a contract or issue a license, grant, security clearance, national security eligibility, credential or accreditation;

(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: investigative material, 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 (including, but not limited to, adjudications, hearings and appeals, continuous evaluation, inspector general functions, counterintelligence, and research, and insider threat programs);

(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 in another 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. Such uses may include, for example 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 matters 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 or identification of bodies;

(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;

(p) 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;

(q) To 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;

(r) To Department of State officials for the purpose of vetting for employee participation in public speaking events, recruitment events, awards, and assignments;

(s) To private U.S. entities operating overseas to communicate threats against them and their employees;

(t) To the Office of the Director of National Intelligence for inclusion in its Scattered Castles system in order to facilitate reciprocity of background investigations and national security eligibility determinations; and

(u) To a court, adjudicative body, or administrative body before which the Department is authorized to appear when (a) the Department; (b) any employee of the Department in his or her official capacity; (c) any employee of the Department in his or her individual capacity where the U.S. Department of Justice ("DOJ") or the Department has agreed to represent the employee; or (d) the Government of the United States, when the Department determines that litigation is likely to affect the Department, is a party to litigation or has an interest in such litigation, and the use of such records by the Department is deemed to be relevant and necessary to the litigation or administrative proceeding.

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 15, 2008). All these standard routine uses apply to Security Records, State-36.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored both in hard copy and on electronic 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. All hard copies of records containing personal information are maintained in secured file cabinets in restricted areas, access to which is limited to authorized personnel only.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: By individual name, personal or biometric identifier, case number, Department building passes, and Social Security number (for other than visitors), as well as by each category of records in the system.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Retention of these records varies depending upon the specific kind of record involved. The retention periods of records maintained in this system of records range from three years for security support records to 100 years for investigation case files. These 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 and outlined here https://foia.state.gov/Learn/RecordsDisposition.aspx. 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; SA-2, Suite 8100; Washington, DC 20522-8100.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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 Foreign Service Institute distance learning course, PA 459, instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly.

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.

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

security investigation. 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 authentication requirements contained in the Office of Management and Budget Circular Memorandum A-130.

The Department of State will store records maintained in this system of records in cloud systems. All cloud systems that provide IT services and process Department of State information must be specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy.

Only information that conforms with Department-specific definitions for FISMA low or moderate categorization are permissible for cloud usage unless specifically authorized by the Cloud Computing Governance Board. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, NIST Federal Information Processing Standards (FIPS) and Special Publication (SP), and Department of State policy and standards.

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; SA-2, Suite 8100; Washington, DC 20522-8100. The individual must specify that he or she wishes Security 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 Security Records include records pertaining to him or her. Detailed instructions on Department of State procedures for accessing and amending records can be found at the Department's FOIA website (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; SA-2, Suite 8100; Washington, DC 20522-8100.

NOTIFICATION PROCEDURES: Individuals who have reason to believe that this system of records may contain information pertaining to themselves should write to following address: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; SA-2, Suite 8100; Washington, DC 20522-8100. The individual must specify that he or she wishes Security Records to be checked. At a minimum, the individual must include: full name (including maiden name, if appropriate) and any other names used; date and place of birth; current mailing address and zip code; 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 Security Records include records to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: 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.

HISTORY: Security Records, State-36, was previously published at 80 FR 77691 and Identity Management System, State-72, was previously published at 71 FR 62653.

Mary R. Avery,

Senior Agency Official for Privacy,

Senior Advisor, Office of Global Information Services,

Bureau of Administration,

Department of State.

[FR Doc. 2018-12872 Filed: 6/14/2018 8:45 am; Publication Date: 6/15/2018]