Billing Code 4710-24

DEPARTMENT OF STATE

[Public Notice: 10393]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: Information in Employee Contact Records is used to develop the official locator directories for all personnel, to communicate with the listed categories of individuals in the event of an emergency in which designated contact information will be used, to communicate with designated emergency contacts or next of kin, for mail forwarding purposes of the employee, and to answer official inquiries regarding the location of an employee.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this modified system of records will be effective upon publication, with the exception of new routine uses (a), (b), and (c) 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, D. C. 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 "Employee Contact Records, State-40" 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; SA-2, Suite 8100; Washington, DC 20522-0208; at Privacy@state.gov, or (202) 663-2215.

SUPPLEMENTARY INFORMATION: The purpose of this modification is twofold: (1) to consolidate two existing records systems (Employee Contact Records, State-40 and Foreign Service Employee Locator/Notification Records, State-12) into a single modified State-40, because the records and system purposes are substantially similar, and (2) to make substantive and administrative changes to a variety of sections. These changes reflect movement to cloud storage, new OMB guidance, and new emergency notification procedures. The modified system of records will include modifications and/or additions to the following sections: Categories of Individuals Covered by the System; Categories of Records in the System; Purpose(s) of 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 Retrieval of Records; and Administrative, Technical, and Physical Safeguards, as well as other administrative updates.

SYSTEM NAME AND NUMBER: Employee Contact Records, State-40.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Department of State ("Department"); 2201 C Street, NW; Washington, DC 20520 and within a government cloud provided, implemented and

overseen by the Department's Enterprise Server Operations Center (ESOC), 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER(S): There are four system managers: (1) Division Chief, Bureau of Administration, Office of Emergency Management, 2430 E Street NW, Washington, DC 20520 on (202) 776-8600; (2) The Chief Information Officer, Bureau of Information Resource Management, Enterprise Resource Management, 2201 C Street, NW Washington, DC 20520. Contact information is either ITServiceCenter@state.gov or (202) 647-2000; (3) Chief, Employee Services Center, Department of State, 2201 C Street, NW, Washington, DC 20520, (202) 647-4054; and (4) Division Chief, A/EX/ITS, Department of State, 600 19th Street, NW, Washington, DC 20431, (202) 485-7147.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301 (Management of the Department of State); 22 U.S.C. 2581 (General Authority of Secretary of State); 22 U.S.C 2651a (Organization of the Department of State); National Security Presidential Directive (NSPD) -51/Homeland Security Presidential Directive (HSPD) - 20 (May 4, 2007); National Continuity Policy Implementation Plan (August 2007); and Federal Continuity Directive 1 (February 2008).

PURPOSE(S) OF THE SYSTEM: The public and non-public information contained in the system is collected and maintained by the Department and is used: (1) to develop the official locator directories for all personnel; (2) to communicate with the categories of individuals listed in the next section in the event of an emergency in which designated contact information will be used; (3) to communicate with designated emergency contacts or next of kin; (4) for mail forwarding purposes of the employee;

and (5) to answer official inquiries regarding the location of an employee.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Foreign and Civil Service employees, U.S. Government employees who fall under a Chief of Mission's (COM) security responsibility; contractors; locally employed staff; employees on intermittent, temporary, and limited appointments; interns; and designated emergency contacts or next of kin to include eligible family members who fall under a Chief of Mission's security responsibility, members of households at overseas posts, and other individuals living/working on Mission property with COM permission who voluntarily agree to provide personal contact information to the Department of State for emergency notification and accountability purposes. Additionally, it includes retired employees. 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 the following contact information, as applicable, for those individuals listed in the preceding section: name, office contact information (current post assignment, employment affiliation, work title, domestic facility location, work address, and work phone numbers), personal contact information (personal phone numbers, personal email address, home address, local address), emergency contact information, employment type, the last four-digits of a Social Security number, Global Employment Management System (GEMS) number, mail forwarding instructions, name of spouse, names of dependents, and school address.

RECORD SOURCE CATEGORIES: The information is compiled directly from the individual and from Department automated sources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Information in Employee Contact Records is used to answer inquiries regarding the location of individuals listed in the Categories of Individuals section. The Department will use the information to notify an emergency contact or next-of-kin in the event of an emergency, crisis or death of the employee, or to contact individuals listed in the categories of individuals section in the event of an emergency at the location where they are assigned abroad to determine if they are safe, or to locate an individual listed in the categories of individuals section in the event of a family emergency or death. The information may also be released to:

(a) Non-governmental agencies or entities during a disaster for purposes of emergency response.

(b) 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.

(c) 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. The 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 the Employee Contact Records, State-40.

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.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrievable by individual's name, dependent name, spouse name and GEMS number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The records retention schedules vary according to function. Some records are transitory in nature and are kept for up to 72 hours while others are kept as long as five years after the employee resigns or retires. These records will

be maintained until they become inactive, at which time they will be retired or destroyed in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration (NARA) and outlined here https://foia.state.gov/Learn/RecordsDisposition.aspx. More specific information may be obtained by writing to: U.S. Department of State; Director, Office of Information Programs and Services; A/GIS/IPS; SA-2, Suite 8100; Washington, DC 20522-0208; or by fax at 202- 261-8571.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All users are given cyber security awareness training that covers the procedures for handling Sensitive But Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Foreign Service and Civil Service employees and those Locally Employed Staff who handle PII 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.

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. While the majority of records covered in the Employee Contact Records are electronic, 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 Employee Contact Records a user must first be granted access to the Department of State computer system. Remote access to the Department of State network from non-Department owned systems is authorized only to unclassified systems and 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. All Department of State employees and contractors with authorized access have undergone a thorough background security investigation.

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 authorized to operate 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 Department's Cloud Computing Governance Board. Prior to operation, all Cloud systems must comply with applicable security measures that are outlined in FISMA, FedRAMP, OMB guidance, NIST Federal Information Processing Standards (FIPS) and Special Publications, and Department of State policy and standards.

RECORD ACCESS PROCEDURES: Individuals who wish to gain access to or to 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 20522-0208. The individual must specify that he or she wishes the Employee Contact 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 Employee Contact Records include records pertaining to him or her. Detailed instructions on Department of State procedures for accessing and amending records can be found 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; SA-2, Suite 8100; Washington, DC 20522-0208.

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; SA-2, Suite 8100; Washington, DC 20522-0208. The individual must specify that he or she wishes the Employee Contact 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 Employee Contact Records include records pertaining to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: The Department of State proposes to consolidate two record systems: Employee Contact Records, State-40 (previously published at 75 FR 67431) and Foreign Service Employee Locator Notification Records, State-12 (previously published at 42 FR 49705).

Mary R. Avery,

Senior Agency Official for Privacy

Senior Advisor, Office of Global Information Services

Bureau of Administration

Department of State

[FR Doc. 2018-08485 Filed: 4/23/2018 8:45 am; Publication Date: 4/24/2018]