Volume 82, Number 237
Tuesday, December 12, 2017
Public Notice 10226; Page 58477

Privacy Act of 1974; System of Record:

Email Archive Management Records, State-01.

SUMMARY: The purpose of the Email Archive Management Records system is to capture all emails and attachments that interact with a Department of State email account and to store them in a secure repository that allows for search, retrieval, and view when necessary.

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 that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by January 4, 2018.

ADDRESSES: Comments 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 Chief Privacy Officer, Margaret P. Grafeld, at Privacy@state.gov. Please write "Email Archive Management Records, State-01" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Margaret P. Grafeld, Chief Privacy Officer; U.S. Department of State; Office of Global Information Services, A/GIS/PRV; SA–2, Suite 8100; Washington, DC 20522-0208.

SUPPLEMENTARY INFORMATION: None.

SYSTEM NAME AND NUMBER: Email Archive Management Records, State-01.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Department of State ("Department'), located at 2201 C Street NW, Washington, DC 20520; Department of State annexes, U.S. Embassies, U.S. Consulates General, and U.S. Consulates. Information may also be

stored within a government-certified cloud, implemented, and overseen by the Department's Messaging Systems Office (MSO), 2025 E. St., N.W., Washington, D.C. 20006.

SYSTEM MANAGER(S): Division Chief, Office of Information Resource Management, Messaging Systems Office, Messaging Design Division; U.S. Department of State, 7049 Newington Rd; Lorton, VA 22079. The System Manager can be reached at (703) 746-2113.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

(a) 5 U.S.C. 301

(b) Federal Records Act, 44 U.S.C. Ch. 31;

(c) Freedom of Information Act, 5 U.S.C. § 552.

(d) Privacy Act of 1974, 5 U.S.C. § 552a(d).

(e) 22 C.F.R. Part 171.

PURPOSE(S) OF THE SYSTEM: The purpose of the system is to capture all emails and attachments that interact with a Department of State email account and to store them in a secure repository that allows for search, retrieval, and view when necessary.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals who maintain a Department of State email account that is archived in the system. The system may also include information about individuals who interact with a Department of State email account, as well as individuals who are mentioned in a Department of State email message or attachment. 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: The records in this system include email messages and attachments associated with a Department of State email account, including any information that may

be included in such messages or attachments. The system may also include biographic and contact information of individuals who maintain a Department of State email account, including name, address, email address, and phone number.

RECORD SOURCE CATEGORIES: These records contain information obtained from individuals who maintain a Department of State email account, as well as those who interact with such individuals.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: The information in the system may be shared with:

(a) other federal agencies, foreign governments, and private entities where relevant and necessary for them to review or consult on documents that implicate their equities;

(b) a contractor of the Department having need for the information in the performance of the contract, but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

(c) 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.

(d) 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.

(e) an agency, whether federal, state, local or foreign, where a record indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, so that the recipient agency can fulfill its responsibility to investigate or prosecute such violation or enforce or implement the statute, rule, regulation, or order.

(f) the Federal Bureau of Investigation, the Department of Homeland Security, the National Counter-Terrorism Center (NCTC), the Terrorist Screening Center (TSC), or other appropriate federal agencies, for the integration and use of such information to protect against terrorism, if that record is about one or more individuals known, or suspected, to be or to have been involved in activities constituting, in preparation for, in aid of, or related to terrorism. Such information may

be further disseminated by recipient agencies to Federal, State, local, territorial, tribal, and foreign government authorities, and to support private sector processes as contemplated in Homeland Security Presidential Directive/HSPD-6 and other relevant laws and directives, for terrorist screening, threat-protection and other homeland security purposes.

(g) a congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

(h) 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.

(i) the Department of Justice ("DOJ") for its use in providing legal advice to the Department or in representing the Department in a proceeding before a court, adjudicative body, or other administrative body before which the Department is authorized to appear, where the Department deems DOJ's use of such information relevant and necessary

to the litigation, and such proceeding names as a party or interests:

(a) The Department or any component of it;

(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 DOJ has agreed to represent the employee; or

(d) The Government of the United States, where the Department determines that litigation is likely to affect the Department or any of its components.

(j) the National Archives and Records Administration and the General Services Administration: for records management inspections, surveys and studies; following transfer to a Federal records center for storage; and to determine whether such records have sufficient historical or other value to warrant accessioning into the National Archives of the United States.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored 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.

POLICIES AND PRACTICES FOR

RETRIEVAL OF RECORDS: By individual name or other personal identifier, if available.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The Department of State is in the process of finalizing a retention schedule for these records. Once the schedule is approved by the National Archives and Records Administration, the Records will be retired in accordance with the published Department of State Records Disposition Schedule that shall be published 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 20522-0208.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All users are given cyber security 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 Employed Staff who handle PII are required to take a 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 Email Archive Management 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 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. 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 Department of State workstations/networks requires a valid PKI identification card protected by a user's PIN that must first be entered before accessing the Department of State network. 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.

The safeguards in the following paragraphs apply only to records that are maintained 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.

Information that conforms with Department-specific definitions for FISMA low, moderate, or high categorization are permissible for cloud usage and must specifically be authorized by the Cloud Computing Governance Board. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud system. The

Email Archive Management Records system is rated as a FISMA high system. In accordance with Department policy, systems that process more sensitive information will require more stringent controls and review by Department cybersecurity experts prior to approval. 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 policies and standards.

All data stored in cloud environments categorized above a low FISMA impact risk level must be encrypted at rest and in-transit using a federally-approved encryption mechanism. The encryption keys shall be generated, maintained, and controlled in a Department data center by the Department key management authority. Deviations from these encryption requirements must be approved in writing by the Authorizing Official. Data in Email Archive Management Records categorized at a high FISMA impact risk level will additionally be subject to continual auditing and monitoring, multifactor authentication mechanisms utilizing PKI, NIST 800-53 controls concerning virtualization, servers, storage and networking as well as stringent measures to sanitize data from the cloud service once the contract is terminated.

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 Email Archive Management 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 Email Archive Management 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 Email Archive Management 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 Email Archive Management Records include records pertaining to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: 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), (k)(3), (k)(4), (k)(5), (k)(6), and (k)(7), 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).

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.

HISTORY: None.