Volume 81, Number 17
Wednesday, January 27. 2016
Public Notice 9425; Page 4736

**Privacy Act; System of Records: Digital Outreach and Communications, State- 79.**

**SUMMARY:** Notice is hereby given that the Department of State proposes to amend an existing system of records, Digital Outreach and Communications, State-79, 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 March 7, 2016, 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 retain the name "Digital Outreach and Communications" (previously published at 78 FR 54946). The purpose of the system is to extend outreach, engagement, and collaboration efforts with the public, and to facilitate transparency and accountability with regard to Department activities; to conduct and administer contests, challenges, and other competitions; and to track aggregate activity and analytics to determine the effectiveness of email campaigns. The proposed system will include modifications to the following sections: System location, Categories of individuals, Categories of records, Authority for maintenance of the system, Purpose, Routine uses, Retrievability, Safeguards, and Notification procedure. The modifications will allow the contact information to be stored in a FEDRAMP Certified Cloud provider, and will allow the Department to collect aggregate activity and analytics of email campaigns.

The Department's report was filed with the Office of Management and Budget. The amended system description, "Digital Outreach and Communications, State-79," will read as set forth below.

Joyce A. Barr,
Assistant Secretary for Administration,
U.S. Department of State.

**STATE-79**

**SYSTEM NAME:**

Digital Outreach and Communications

**SECURITY CLASSIFICATION**:
Unclassified

**SYSTEM LOCATION:**
Department of State domestic locations, posts abroad, and within a government cloud, implemented by State Department as a cloud-based cloud software as a service (SaaS) provider.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**
Individuals who interact with the Department through a social media outlet, or other electronic means including by submitting feedback, subscription (RSS), email, requesting more information from the Department. Individuals participating in a contest, challenge, or other competition.

**CATEGORIES OF RECORDS IN THE SYSTEM:**
The system may contain information passed through a social media site or cloud service provider to facilitate interaction with the Department such as, but not limited to the following: name, username, e-mail address, home or work address, contact information, phone numbers, date of birth, age, security questions, IP addresses, login credentials, topical interests, and educational, business, or volunteer affiliation. The system will also contain information on the topics about which users wish to receive communications, as well as input and feedback from the public, such as comments, e-mails, videos, and images, which may include tags, geotags, or geographical metadata. The system may also include information that does not meet the definition of a "record" under the Privacy Act, such as aggregate metrics on user click rates, open rates, non-read rates, unsubscribes, and link activity.
In addition to the information listed above, individuals who enter a contest, challenge, or other competition may be asked to provide certain specific information including financial data, passport and visa information, and other information necessary to authenticate qualifications for participation or for prize issuance.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**
Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009. OMB M-10-06, Open Government Directive, December 8, 2009. OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010. 5 U.S.C. 301, Management of Executive Agencies. 22 U.S.C. 2651a, Organization of the Department of State.

**PURPOSE:**

To extend outreach, engagement, and collaboration efforts with the public, and to facilitate transparency and accountability with regard to Department activities. To conduct and administer contests, challenges, and other competitions. To track aggregate activity and analytics to determine the effectiveness of email campaigns.

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

Information in this system may be shared with the news media and the public, with the approval of the Chief of Mission or Bureau Assistant Secretary who supervises the office responsible for the outreach effort, except to the extent that release of the information would constitute an unwarranted invasion of personal privacy;

To Government agencies and the White House for purposes of planning and coordinating public engagement activities;

To 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);

And to Federal, state, and city governments which are issued tax reports, the Internal Revenue Service and the Social Security Administration which are sent tax and withholding data.

The Department of State periodically publishes in the Federal Register its standard routine uses which 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 Digital Outreach and Communications, State-79.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

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

**STORAGE:**

Electronic media.

**RETRIEVABILITY:**

Username; email; name.

**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 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 only. 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 Digital Communication and Outreach, 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 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. 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: (1) provisionally authorized to operate by the Federal Risk and Authorization Management Program (FedRAMP), and (2) specifically authorized by the Department of State Authorizing Official and Senior Agency Official for Privacy. Only information that conforms with Department-specific definitions for Federal Information Security Management Act (FISMA) low or moderate categorization are permissible for cloud usage. Specific security measures and safeguards will depend on the FISMA categorization of the information in a given cloud 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 policy 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.

**RETENTION AND DISPOSAL:**

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). 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(S) AND ADDRESS:**

The Under Secretary for Public Diplomacy and Public Affairs; Department of State; 2201 C Street NW; Washington, DC 20520.

**NOTIFICATION PROCEDURE:**

Individuals who have cause to believe that the Department may have outreach records pertaining to him or her 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 or she wishes the outreach records of the Department to be checked. At a minimum, the individual must include the following: name; email address; current mailing address and zip code; signature; and other information helpful in identifying the record.

**RECORD ACCESS 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:**

Individuals who wish to contest records pertaining to themselves should write to the Director; Office of Information Programs and Services (address above).

**RECORD SOURCE CATEGORIES:**

These records contain information obtained directly from individuals who interact with the Department of State through social media sites or who communicate electronically

with the Department in response to public outreach.

**SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT**:

None.