Volume 82, Number 237
Tuesday, December 12, 2017
Public Notice 10225; Page 58475

Privacy Act of 1974; System of Record:

Network User Account Records,

State-56.

SUMMARY: This System of Records compiles information about Department of State user accounts to monitor and control access to Department of State networks and computer systems.

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 (a) and (b) that are subject to a 30-day period during which interested persons may submit comments to the Department. Please submit any comments by January 11, 2017.

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 Chief Privacy Officer, Margaret P. Grafeld, at Privacy@state.gov. Please write "Network User Account Records, State-56" 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: The purpose of this modification is to make substantive and administrative changes to the the previously published notice. This notice modifies the following sections of State-56, Network User Account Records: System Location, Categories of Individuals, Routine Uses, Storage, 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 Department’s move to cloud storage, new OMB guidance,

access by contractors, updated contact information, and a notice publication history.

SYSTEM NAME AND NUMBER: Network User Account Records, State-56.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Department of State ("Department"), located at 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): Chief Information Officer, Bureau of Information Resource Management, Department of State, 2201 C Street, NW, Washington, DC 20520 and can be reached at either ITServiceCenter@state.gov or (202) 647-2000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 44 U.S.C. 3544.

PURPOSE(S) OF THE SYSTEM: To administer Department network user accounts; to help document and/or control access to computer systems, platforms, services, applications, and databases within a Department network and Department-authorized cloud services and applications; to monitor security of computer systems; to investigate and make referrals for disciplinary or other actions if unauthorized access or inappropriate usage is suspected or detected; and to identify the need for training programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Department of State employees and other organizational users (examples include eligible family members, locally employed staff, contractors, and personal services contractors) who have access to Department of State computer networks and access to cloud computing applications that are authorized for

processing Department information. 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 of records consists of the network and application user account records that Department information technology systems, applications, and services compile and maintain about users of a network and application. These records include user data such as the user's name, system-assigned username; e-mail address; employee or other user identification number; organization code; job title; business affiliation; work contact information; systems, applications, or services to which the individual has access; systems, applications, or services used; dates, times, and durations of use; profile photo; user profile; and IP address of access. The records also include system usage files and directories when they contain information about specific users.

RECORD SOURCE CATEGORIES: Individuals about whom the network user account record is maintained; information technology systems, applications, and services within a Department network that record usage by individuals assigned a user account on that network.

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

(a) To 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.

(b) 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.

The Department of State periodically publishes in the Federal Register its standard routine uses which apply to many 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 Network User Account Records, State-56.

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 in the Department's Foreign Affairs Manual (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 indexed by the name; system-assigned username; e-mail address; or other searchable data fields or codes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records maintained in this system of records are generally destroyed three to six years after the user account is terminated. These 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), and a complete list of the Department's schedules can be found on our Freedom of Information Act (FOIA) program's website (https://foia.state.gov/Learn/RecordsDisposition.aspx). More specific information may be obtained by writing to the following address: Director, Office of Information Programs and Services, A/GIS/IPS; SA–2, Department of State; 515 22nd Street NW; Washington, DC 20522-8100.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All users are given cyber security awareness training that 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 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 Network User Account 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 Network User Account 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 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 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 Network User Account 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 Network User Account 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 20522-0208.

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 Network User Account 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 Network User Account Records include records pertaining to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: This SORN was previously published at 75 FR 7210.