Billing Code 4710-24

DEPARTMENT OF STATE

[Public Notice: 10126]

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a New System of Records.

SUMMARY: Ombudsperson Mechanism Records includes information about individuals who have submitted requests relating to national security access to data transmitted to the United States pursuant to the Privacy Shield Framework Ombudsperson Mechanism and any similar mechanism established between the United States and another country or countries. The system assists in the overall management of the request review process and the provision of responses thereto by facilitating accurate and up-to-date record keeping.

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 [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 Chief Privacy Officer, Margaret P. Grafeld, at Privacy@state.gov. Please

write "Ombudsperson Mechanism Records, State-83" 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: Ombudsperson Mechanism Records, State-83.

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): International Communication and Information Policy Officer for Europe, Office of Communications & Information Policy, Bureau of Economic and Business Affairs; U.S. Department of State, 2201 C St. Washington, DC 20520. System Managers can be reached at (202) 647-8784.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: (a) State Department Basic Authorities Act of 1956, as amended (22 U.S.C. 2708 et seq.); (b) Privacy Shield Framework (81 Fed. Reg. 51042).

PURPOSE(S) OF THE SYSTEM: The EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework create a mechanism for companies on both sides of the Atlantic to comply with EU data protection requirements when transferring personal data from the European Union and Switzerland, respectively, to the United

States in support of transatlantic commerce. The Frameworks each established an Ombudsperson Mechanism to address appropriate inquiries by individuals relating to U.S. Intelligence Community access to personal data transmitted from the EU or Switzerland to the United States through Privacy Shield and related commercial transfer mechanisms. The information will be used by the Ombudsperson to ensure that requests are properly investigated and addressed in a timely manner, and that the relevant U.S. laws have been complied with or, if the laws have been violated, that the situation has been remedied.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals whose requests relating to national security access to data transmitted from the European Union to the United States under the Privacy Shield Framework (81 Fed. Reg. 51042), and the EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence ("Ombudsperson Mechanism") thereunder, are submitted by the "EU individual complaint handling body" to the Department. Individuals who submit requests relating to national security access to data transmitted under any similar mechanism established between the United States and another country or countries. 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: These records may include biographic and contact information, such as name, address, email address, phone number, and information about residency or nationality, as well as other information that requesters and foreign government officials include in the requests submitted to the

Department. The records also may include information about an individual's request and the processing of that request.

RECORD SOURCE CATEGORIES: Individuals who submit requests for review under the Privacy Shield Ombudsperson Mechanism or similar arrangement are the primary source of record information, although that information is provided to the Department by the EU Individual Complaint Handling Body or corresponding body under similar arrangements. Additional information necessary to process individual requests may be provided by these bodies as well as other federal agencies.

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

A. To other Federal Agencies or bodies to facilitate the consideration, processing and resolution of requests consistent with Section 2 of the Ombudsperson Mechanism (accessed via https://www.state.gov/e/privacyshield/ombud/).

B. To an EU individual complaint handling body and any other complaint handling body established under a similar arrangement with another country to coordinate the discharge of commitments made therein. For example, the Privacy Shield Ombudsperson will communicate directly with the EU individual complaint handling body regarding requests submitted pursuant to the Ombudsperson Mechanism for reasons including acknowledging receipt of the request from the EU individual complaint handling body, requesting additional information necessary to perfect the request, and providing a final response. The EU individual complaint handling body will in turn be responsible for all communications with individuals who submit requests.

C. 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).

D. 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.

E. 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.

F. To 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.

G. To 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.

H. To 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.

I. 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.

J. To 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.

K. To 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 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/05 FAM0440.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 or other personal identifier, if available, and by a tracking number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The Department of State is in the process of developing 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 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 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 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 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. Before being granted access to Ombudsperson Mechanism Records, a user must first be granted access to the Department of State computer system.

Department of State employees and contractors may remotely access this system of records using non-Department owned information technology. Such access is subject to approval by the Department's access program, and is limited to information maintained in unclassified information systems. Remote access to the Department's information

systems is configured in compliance with OMB Circular A-130 multifactor authentication requirements and includes a time-out function.

All Department of State employees and contractors with authorized access to records maintained in this system of records 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. While the majority of records in Ombudsperson Mechanism will be in an electronic format, paper mailings from the EU individual complaint handling body could be included in the system. 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.

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. The categorization of information in this system of records is designated as low. 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 Ombudsperson Mechanism 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 Ombudsperson Mechanism 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 Ombudsperson Mechanism 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 Ombudsperson Mechanism Records include records pertaining to him or her.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

Mary R. Avery,

Senior Agency Official for Privacy

Senior Advisor, Office of Global Information Services

Bureau of Administration

Department of State

[FR Doc. 2017-19818 Filed: 9/15/2017 8:45 am; Publication Date: 9/18/2017]