

Department of State

STATE-84 Secretariat Contact Records

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a New System of Records.

SUMMARY: Information in Secretariat Contact Records is used to facilitate Department communication with domestic and foreign interlocutors.

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, email or by calling John C.

Sullivan, the Senior Agency Official for Privacy, on (202) 647-6435. If mail, please write to: U.S Department of State; Office of Global Information Systems; A/GIS; Room, 1417, 2201 C St., N.W.; Washington, DC 20520. If email, please address the email to the Senior Agency Official for Privacy, John C. Sullivan, at Privacy@state.gov. Please write "Secretariat Contact Records, State-84" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION

CONTACT: John C. Sullivan, Senior Agency Official for Privacy; U.S.

Department of State; Office of Global Information Services, A/GIS; Room 1417, 2201 C. St., N.W.; Washington, DC 20520 or by calling (202) 647-6435.

SUPPLEMENTARY INFORMATION:

None.

SYSTEM NAME AND NUMBER:

Secretariat Contact Records, State-84.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION: Department of State (“Department”), located at 2201 C Street NW, Washington, DC 20520.

SYSTEM MANAGER(S): Director, Operations Center, 2201 C Street NW, Washington, DC 20520, operationscenter@state.gov, (202) 647-1512.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 8 U.S.C. 1104 (Powers and Duties of the Secretary of State).

PURPOSE(S) OF THE SYSTEM: Information in the Secretariat Contact Records is used to facilitate Department communication with domestic and foreign interlocutors. These records are maintained by the Operations Center staff and used to establish calls when needed by the Secretary of State to discuss foreign policy matters.

Additional data is collected in the form of call notes that help clarify contact

methods.

CATEGORIES OF INDIVIDUALS

COVERED BY THE SYSTEM:

Individuals who interact with Department of State officials on matters of official business. 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: Contact information related to individuals who interact with Department of State officials on matters of official business. These records include name, email addresses, phone numbers, and job title.

These records may also include information about the individual’s previous interactions with the Department of State, such as the purpose and date of a call connected by the Department of State’s Operations Center and notes to clarify contact methods for the individual.

RECORD SOURCE CATEGORIES:

These records contain information that is

primarily obtained from the individual who is the subject of the records.

**ROUTINE USES OF RECORDS
MAINTAINED IN THE SYSTEM,
INCLUDING**

**CATEGORIES OF USERS AND
PURPOSES OF SUCH USES:** Secretariat

Contact 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.
- (c.) 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.) 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.
- (e.) 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.

- (f.) 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.
- (g.) 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.

- (h.) 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 as 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.

- (i.) 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: Secretariat Contact

Records information is retrieved almost exclusively through a name or phone number search. Other fields, such as address or title, are available for retrieval, but are rarely used.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

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 outlined here

<https://foia.state.gov/Learn/RecordsDisposition.aspx>.

Secretariat Contact Records are governed by Records Schedule A-03-006-10 which covers temporary customer/client records that may be deleted when they are superseded,

become obsolete or the customer/client requests the agency remove the records.

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; 2201 C Street, N.W.; Room B-266; Washington, DC 20520.

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 the Foreign Service Institute's 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. 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 Secretariat 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 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.

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; 2201 C Street, N.W; Room B-266; Washington, DC 20520. The individual must specify that he or she wishes the Secretariat 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 Secretariat 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 the
Department's FOIA website located 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; 2201 C Street, N.W.; Room B-
266; Washington, DC 20520.

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; 2201 C Street, N.W.;
Room B-266; Washington, DC 20520. The
individual must specify that he or she
wishes the Secretariat 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 Secretariat Contact
Records include records pertaining to him
or her.

EXEMPTIONS PROMULGATED FOR

THE SYSTEM: None.

HISTORY: None

Eric F. Stein,
Senior Agency Official for Privacy,
Acting Deputy Assistant Secretary,
Office of Global Information Services,
Bureau of Administration,
Department of State.