Volume 87, Number 56
Wednesday, March 23, 2022
Public Notice 11688; Page 16542

Privacy Act of 1974; System of Records: Risk Analysis and Management Records

Department of State

Privacy Act of 1974; System of Records

AGENCY: Department of State.

ACTION: Notice of a Modified System of Records.

SUMMARY: The information in this system of records, Risk Analysis and Management Records, supports the vetting of directors, officers, or other employees of organizations who apply for Department of State contracts, grants, cooperative agreements, or other funding; and individuals who may benefit from such funding. The information collected from these organizations and individuals is specifically used to conduct screening to ensure that Department funds are not used to provide support to entities or individuals deemed to be a risk to U.S. national security interests.

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), (b), (c), (d), and (e) 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 Eric F. Stein, the Senior Agency Official for Privacy on (202) 485-2051. 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, Eric F. Stein, at Privacy@state.gov. Please write "Risk

Analysis and Management Records, State-78" on the envelope or the subject line of your email.

FOR FURTHER INFORMATION CONTACT: Eric F. Stein, 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 on (202) 485-2051.

SUPPLEMENTARY INFORMATION: This notice is being modified to reflect new OMB guidance, changes to the categories of records and security classification. The modified system of records notice includes substantive revisions and additions to the following sections: Dates, Security Classification, System Location, Categories of Individuals Covered by the System, Categories of Records in the System, Routine Uses of Records, Retention and Disposal of Records, and Exemptions Promulgated. In addition, the Department is taking this opportunity to make minor administrative updates to the following sections: Addresses, For Further Information Contact, and History.

SYSTEM NAME AND NUMBER: Risk Analysis and Management Records, State-78.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Office of Risk Analysis and Management (RAM), Department of State, Washington, D.C., 2201 C St., N.W., Washington, DC 20520.

SYSTEM MANAGER(S): Director, Office of Risk Analysis and Management (RAM) 2201 C St., N.W., Washington, DC 20520, RAM@state.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 18 U.S.C. 2339A, 2339B, 2339C; 22 U.S.C.2151 et seq.;

Executive Orders 13224, 13099 and 12947; and Homeland Security Presidential Directive-6.

PURPOSE(S) OF THE SYSTEM:

The information in the system supports the vetting of directors, officers, or other employees of organizations who apply for Department of State contracts, grants, cooperative agreements, or other funding; and individuals who may benefit from such funding. The information collected from these organizations and individuals is specifically used to conduct screening to ensure that Department funds are not used to provide support to entities or individuals deemed to be a risk to U.S. national security interests.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The system covers key personnel of organizations that have applied for contracts, grants, cooperative agreements, or other funding from the Department of State; and individuals who may benefit from such funding. These individuals may include but are not limited to principal officers or directors, program managers, chief of party for the program and other individuals employed by the organization. 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: Information in this system includes: name, aliases, date and place of birth, gender (as shown in a government-issued foreign or U.S. photo ID), citizenship(s), government-issued identification information (including but not limited to Social Security number if U.S. citizen or Legal Permanent Resident, passport number, or any other numbers originated by a government that specifically identifies an individual), mailing address, telephone numbers, e-

mail, social media information, current employer organizational and project title.

RECORD SOURCE CATEGORIES: Information is collected from the record subjects themselves and also from public sources, agencies conducting national security screening, law enforcement and intelligence agency records, and other government databases.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: Risk Analysis and Management 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.) To other U.S. government agencies for vetting programs.

(d.) 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.

(e.) To a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to

obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

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 Risk Analysis and Management Records, State-78.

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 at 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 only.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name, date and place of birth, government identifying numbers (such as Social Security numbers or passport numbers), or other identifying data specified under Categories of Records in the system.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records with no derogatory findings are purged annually; records with derogatory information are

maintained for seven years. 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 at 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; 2201 C Street, N.W., Room B-266; Washington, DC 20520.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: All Department of State network 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 Department OpenNet network users are required to take, on a biennial basis, 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 Risk Analysis and Management Records, a user must first be granted access to the Department of State computer network.

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 mobile and remote 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. 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.

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 Risk Analysis and 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 Risk Analysis and

Management Records include records pertaining to the individual. 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 a record 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 themselves 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 Risk Analysis and 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 Risk Analysis and Management Records include records pertaining to the individual.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: To the extent applicable, because this system contains information related to the government's national security programs, records in this system may be exempt from any part of 5 U.S.C 552a except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6),(7),

(9), (10), and (11) if the records in the system are subject to the exemption found in 5 U.S.C. 552a(j). To the extent applicable, records in this system may be exempt from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a if the records in the system are subject to the exemption found in 5 U.S.C. 552a(k). Any other exempt records from other 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: Previously published at 76 FR 76215.