Volume 76, Number 234
Tuesday, December 6, 2011
Public Notice 7709

**STATE-78**

**SYSTEM NAME:**

Risk Analysis and Management (RAM) Records.

**SECURITY CLASSIFICATION:**

Classified and Unclassified.

**SYSTEM LOCATION:**

Department of State, 2201 C Street NW, Washington, DC 20520; other Department of State annexes, posts and missions abroad; and the United States Agency for International Development (USAID), Office of Security, 1300 Pennsylvania Avenue NW, Washington, DC 20523.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

The system covers key personnel of organizations who have applied for contracts, grants, cooperative agreements or other funding from the Department of State. 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.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Unclassified information in this system includes, but is not limited to: 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 number(s), fax number, email address, current employer and job title. The type of grant, U.S. dollar value of contract/grant, the contract/grant start and end date, and the purpose of the contract/grant are also contained in the system.

Classified information in this system includes, but is not limited to: results generated from the screening of individuals covered by this Notice; intelligence and law enforcement information related to national security; and national security vetting and terrorism screening information provided to the Department by other agencies.

**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:**

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. 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.

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

Information may be disclosed to the United States Agency for International Development (USAID) and to federal government agencies for vetting programs. 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 State-78, Risk Analysis and Management Records.

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

**STORAGE:**

Records in this system are stored in both paper and electronic format.

**RETRIEVABILITY:**

Records are retrieved by name, date and place of birth, government-issued identifying numbers (such as Social Security numbers or passport numbers), and solicitation number.

**SAFEGUARDS:**

The records are maintained in an authorized security container with access limited to authorized government personnel and authorized contractors. Physical security protections include guards and locked facilities requiring badges. Only authorized government personnel and authorized contractors can access records within the system. The Department mandates and certifies that physical and technological safeguards appropriate for classified and Sensitive but Unclassified systems are used to protect the records against unauthorized access.

All authorized government personnel and authorized contractors with access to the system must hold an appropriate security clearance, sign a non-disclosure agreement, and undergo both privacy and security training.

Classified and Sensitive but Unclassified paper records are kept in an approved security container. Access to these records is limited to those authorized government personnel and authorized contractors who have a need for the records in the performance of their official duties.

Electronic records are kept in a secure database. Access to the records is restricted to those authorized government personnel and authorized contractors with a specific role in the vetting process as part of the performance of their official duties. The RAM database is housed on and accessed from a Sensitive but Unclassified computer network. Vetting requests, analyses, and results will be stored separately on a classified computer network. Both computer networks and the RAM database require a user identification name and password and approval from the Office of Security. An audit trail is maintained and periodically reviewed to monitor access to the system. When it is determined that a user no longer needs access, the user account is disabled.

Authorized government personnel and authorized contractors assigned roles in the vetting process are provided role-specific training to ensure that they are knowledgeable in how to protect personally identifiable information. Access to the Department of State records within the system will be controlled by the network firewall configuration.

Within the Department of State, 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 Engaged Staff who handle PII are required to take the FSI 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 RAM 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 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.

**RETENTION AND DISPOSAL:**

Records are retired 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 the Director; Office of Information Programs and Services, A/GIS/IPS; Department of State, SA-2; 515 22nd Street, NW, Washington, DC 20522-8001.

**SYSTEM MANAGER(S) AND ADDRESS:**

Office of Risk Analysis and Management, Department of State, Washington, DC, 2201 C St. NW, Washington, DC 20520.

**NOTIFICATION PROCEDURE:**

Individuals who have cause to believe that Risk Analysis and Management Records might have records pertaining to them should write to the Director; Office of Information Programs and Services, A/GIS/IPS, Department of State, SA-2; 515 22nd Street NW, Washington, DC 20522-8001. The individual must specify that he/she wishes the records of the Risk Analysis and Management Records to be checked. At a minimum, the individual must include: name; date and place of birth; current mailing address and zip code; signature; and the approximate dates of application for a contract, grant or other funding.

**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:**

See above.

**RECORD SOURCE CATEGORIES:**

Information in this system is obtained from the application form completed and submitted by an organization or individual applying for a contract, grant, cooperative agreement, or other funding from the Department of State. In the case of applications submitted by an individual in his/her own capacity, the information will be collected directly from the individual applicant. Information in this system may also be obtained from public sources, agencies conducting national security screening law enforcement and intelligence agency records, and other government databases.

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

Pursuant to 5 U.S.C. 552a(j)(2), records in this system may be exempt from subsections (c)(3) and (4), (d), (e)(1), (2) and (3), (e)(4)(G), (H), and (I), (e)(5) and (8), (f), (g) and (h) of the Privacy Act. Pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), records in this system may be exempt from subsections 5 U.S.C. 552a(c)(3),(d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act.

If a record contains information from other exempt systems of records, the Department of State will rely on the exemptions claimed for those systems.