STATE-XX (ITAP # to be provided)

SYSTEM NAME:

Risk Analysis and Management (RAM)

SECURITY CLASSIFICATION:

Classified and Sensitive but Unclassified.

SYSTEM LOCATION:

The United States Department of State, 2201 C Street, N.W., Washington, D.C., 20520, other Department of State locations, and the United States Agency for International Development (USAID), Office of Security, 1300 Pennsylvania Avenue, Washington, DC 20523.

USAID will host the electronic records system for the office of Risk Analysis and Management (RAM) in a USAID-managed database. All access and controls to the system will be established by the RAM Program office in coordination with USAID.

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 United States Department of State. These individuals may include:

1. Principal Officers or Directors, including the President, Vice President, Chief Executive Officer, Chief Operating Officer, Treasurer, and Secretary of the organization's governing body (Board of Directors or Board of Trustees).
2. Principal Officers, including Deputy Principal Officer, Executive Director, Deputy Director, President, and Vice President of the organization.
3. Program Manager or Chief of Party for the USG-financed program.

4. Other individuals employed by the organization seeking funding with a role in the State Department financed program.

CATEGORIES OF RECORDS IN THE SYSTEM:

Sensitive but Unclassified and non-exempt identifying information in this system includes, but is not limited to:

Name, 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 US 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 address, current employer and job title.

Classified and exempt information in this system includes, but is not limited to:

1. Results generated from the screening of individuals covered by this notice;
2. Intelligence and law enforcement information related to national security; and
3. 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 purposefully or inadvertently 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:

The information is used to assist the Department in evaluating applications for funding. The Department of State periodically publishes in the Federal Register its standard routine uses that 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 this system of records. State-XX (ITAP# to be provided)

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

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. Paper records are maintained by the Department of State offices when information cannot be collected electronically. Electronic storage is on servers (hard disk media) and magnetic tapes (or other backup media) stored within a security location within the USAID Washington headquarters.

RETRIEVABILITY:

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.

SAFEGUARDS:

The electronic system will be maintained by USAID on its database which is safeguarded as described in the USAID System of Records notice of July 17, 2007, 72 Fed. Reg. 39042. Access to the State Department records within that system will be controlled by firewalls.

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 (LES) 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. 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. 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.

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, Department of State, SA-2, 515 22nd Street NW, Washington, DC 20522-8001.

SYSTEM MANAGER(S) AND ADDRESS:

Risk Analysis and Management, Department of State, Washington, D.C., 2201 C St., N.W., Washington, DC 20520.

NOTIFICATION PROCEDURE:

Individuals who have cause to believe that the Risk Analysis and Management System might have records pertaining to them should write to the Director, Office of Information Programs and Services, 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 System to be checked. At a minimum, the individual must include: name; date and place of birth; current mailing address and zip code; signature; 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 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:

To the extent applicable, because this system contains classified 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. Rules have been promulgated in accordance with the requirements of 5 U.S.C. 553(b), (c), and (e).