



Privacy Impact Assessment
Risk Analysis and Management

Risk Analysis and Management (RAM) PIA

1. Contact Information

Department of State Privacy Coordinator
Sheryl Walter
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- (a) Date PIA was completed: July 2013
- (b) Name of system: Risk Analysis and Management (RAM)
- (c) System acronym: RAM
- (d) IT Asset Baseline (ITAB) number: 7233
- (e) System description:

The RAM program is a State Department effort to enhance our review of organizations, entities and individuals seeking U.S. government funding from the State Department through contracts, grants or other funding instruments. This program will utilize a centralized database to support the vetting of “key employees” of organizations, entities or individuals who apply to the Department of State for contracts, grants or other funding. The information collected is used to conduct screenings to mitigate the risk that Department of State funds could be used to provide support to entities or individuals deemed to be a risk to national security.

- (f) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security re-certification
- (g) Explanation of modification (if applicable): N/A
- (h) Date of previous PIA (if applicable): N/A

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Organizations, entities or individuals seeking contracts, grants or other funding from the Department of State may be required to provide personally identifiable information (PII) on their foreign national and U.S. citizen “key personnel.” Information collected will include the name, date and place of birth, gender, citizenship(s), and government

Risk Analysis and Management (RAM) PIA

identification numbers, such as U.S. passport or Social Security numbers (if U.S. citizen or Legal Permanent Resident), address, telephone and fax numbers, and e-mail address. Some information will be entered into government and public databases for name checks, and other information may be used to help confirm identity, if necessary.

All PII listed is necessary to the vetting procedure. Reducing the amount of PII collected would make it difficult to rule out individuals not properly associated with derogatory information, also called “false positives”.

b. How is the information collected?

Information is obtained directly from the organization, entity or individual. The organization, entity or individual seeking funding obtains all of the information on the Risk Assessment Information form DS-4184 and submits it to RAM directly via paper or electronic submission through a secure portal.

c. Why is the information collected and maintained?

Information is collected to support vetting of “key personnel” of organizations who submit proposals to the Department for contracts, grants, or other funding. It is specifically used to conduct screening to mitigate the risk that Department of State funds could be used to provide support to entities deemed to be a risk to national security.

d. How will the information be checked for accuracy?

Accuracy of the information form is the responsibility of the organization, entity or individual seeking funding.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The Department of State awards contracts, grants and other funding pursuant to a number of legal authorities including the Foreign Assistance Act of 1964, as amended, 22 U.S.C. 2151 et seq.; the Arms Export Control Act, as amended, 22 U.S.C. 2751, et seq.; the Migration and Refugee Assistance Act, 22 U.S.C. 2601 et seq.; and various acts appropriating funds to carry out these authorities. These acts place responsibility in the Secretary of State to implement appropriate measures to ensure that funds are used for the appropriate and authorized purpose and that the programs undertaken using these funds are not contrary to the national security and foreign policy of the United States. Other provisions of law restricting the provision of material support to terrorists or other entities that threaten U.S. national security and foreign policy provide support for the Department’s effort to mitigate the risk that U.S. government funding could go to organizations or individuals that pose a risk to the United States. See, 18 U.S.C. 2339A, 2339B and 2339C. Also see Executive Orders 13224, 13099, and 12947, as well as Homeland Security Presidential Directive- 6.

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Requiring submission of PII carries the inherent risk that it will be revealed, either knowingly or inadvertently, to those without the authority or need for its provision. To mitigate this risk RAM has designed and enabled a “Secure Portal” that allows the individual or organization providing the PII to directly input the data into the system and

Risk Analysis and Management (RAM) PIA

transmit it securely only to RAM where only those USG officials authorized to receive and review the data may access it. All RAM employees authorized to access PII are trained in its proper use and in the required safeguards to prevent unauthorized revelation of the information. In addition, RAM's system has a records maintenance policy that purges the system of all PII on a regular schedule.

4. Uses of the Information

a. Describe all uses of the information.

The Department of State will collect this information in order to support the vetting of directors, officers or employees of non-governmental organizations who apply to the Department of State for contracts, grants or other funding. The information collected from the individuals is specifically used to conduct screening to ensure that State funded activities are not purposefully or inadvertently used to provide support to entities or individuals deemed to be a risk to national security.

b. What types of methods are used to analyze the data? What new information may be produced?

RAM analysts review all of the information provided on the information form together with any additional information received through the name check process. No new information will be produced by RAM.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

RAM analysts review information collected from commercial, public, and U.S. government databases to determine its applicability to the entity or individual seeking funding, and to evaluate whether funding such an entity or individual presents an unacceptable risk to U.S. national security.

d. Is the system a contractor used and owned system?

The system is owned, maintained and operated by Department of State employees and contractors.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Information collected in RAM is used for very limited purposes, described in section 4(a). Direct RAM database access is restricted to cleared server administrators. All access is performed through the RAM application whose connection details are not known by the users. In addition, RAM employs "role-based" controls in which the "Administrator" can grant or deny access to users. All other RAM users will have the ability to create and process vetting requests, delete them from the system, upload files, and view all vetting activity in the system.

5. Retention

a. How long is information retained?

Risk Analysis and Management (RAM) PIA

“Yea” decisions will be deleted/destroyed one year after a contract or grant is awarded.
“Nay” decisions will be deleted/destroyed seven years after a final decision.

Organizations and businesses applying for Department of State funds submit the DS-4184 Information Form. The information will be destroyed after the information has been converted to an electronic medium and verified, when no longer needed for legal or audit purposes or to support the reconstruction of or serve as a backup to the electronic records, whichever is later.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Data is retained on a set schedule of one year for “yea” decisions and seven years for “nay” decisions. This allows for better control and accuracy of the information and ensures that it will not be unnecessarily retained indefinitely.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

If information indicating a possible threat or risk is received from government or public databases, the information will be shared with high level Department of State officials who will make the decision to approve or deny the funding application based on national security risks.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

For internal sharing we use the Department’s Sensitive but Unclassified e-mail system. If the e-mail contains PII, we designate it with a “PII” marking.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing of PII collected in RAM carries the risk of inadvertent or witting disclosure by those outside of RAM who review the data to those not authorized to have knowledge of the information. This risk is mitigated by internal RAM procedures that ensure sharing of PII only with those officials empowered to act on it to prevent provision of State Department funds to people or organizations that might threaten national security. As a practical matter this means that only those files containing “derogatory” information on an organization or individual would be shared, and even then only the nature of the derogatory information would be provided to the decision makers in a bureau considering funding that person or organization. The PII itself would rarely if ever be revealed to the decision maker.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Risk Analysis and Management (RAM) PIA

Information may be shared with other government agencies to the extent necessary to complete the screening process. If negative information exists about key individuals, that information could be shared as part of our routine uses with other U.S. government agencies, including coordination with USAID or other agencies furnishing foreign assistance. (For a complete list of routine uses, please see the system of records notice (SORN) entitled Risk Analysis and Records Management, State-78). Only personnel with specific roles in support of vetting or vetting related decisions would be provided access to the data.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information shared with other U.S. government agencies will be sent through e-mails or paper files marked PII and will be shared only on a need-to-know basis.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Strict controls are in place to protect PII when sharing externally. Information is only shared on a need-to-know basis.

8. Notice

The system:

- contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records:
Risk Analysis and Records Management, State-78
- does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice that information will be collected will be provided when a solicitation is announced. This system does not collect personal information directly from the individuals if an organization or entity is seeking funding. If an individual is seeking funding, that individual will provide the information. Additionally, the DS-4184 has a Privacy Act notice, and notice is provided by the publication of STATE-78.

b. Do individuals have the opportunity and/or right to decline to provide information?

Individuals have the opportunity to decline to provide information. However, if the information is considered to be necessary due to the risk profile of the program, organizations, entities or individuals seeking funding will not be considered eligible for the contract, grant or other funding, unless they provide this information.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Risk Analysis and Management (RAM) PIA

No. The information is needed to undertake screening against other governmental and public databases and to be evaluated in the decision-making process for awarding government funding.

- d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.**

Notice that information will be collected will be provided when a solicitation is announced. The Department of State maintains all classified records in an authorized security container with access limited to authorized government personnel and authorized contractors, and there is no greater risk of privacy than normal. Additionally, State-78 was published to alert the public of the collection of PII for the purposes stated within this PIA.

9. Notification and Redress

- a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?**

Individuals should review submissions, and if errors are noted they should contact the person in their organization who submitted their information to RAM. The office or individual that provided the information is responsible for correcting any misinformation and for resubmitting it to RAM.

- b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.**

Individuals who review their personal information submitted by their organization are at low risk for having incorrect information submitted to RAM. Incorrect information may be corrected and resubmitted to RAM.

10. Controls on Access

- a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

The Department of State maintains all classified records in an authorized security container with access limited to authorized government personnel and authorized contractors. The Department 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 appropriate security clearance, sign a non-disclosure agreement, and undergo both privacy and security training such as the Cyber security Awareness online course.

To access the system, users must be authorized users of the Department of State's unclassified network. Access to RAM data held in the RAM database requires a unique user account assigned by a supervisor. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user

Risk Analysis and Management (RAM) PIA

access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

- a. For paper records: Classified and Sensitive but Unclassified records are kept in an approved security container. Access is limited to those authorized government personnel and authorized contractors who have a need for the records in the performance of their official duties.
- b. For electronic records: Records are kept in a secure database. Access to records is restricted to those authorized government personnel and authorized contractors with a specific role in the vetting process. The Department of State RAM database is housed on and accessed from a Sensitive but Unclassified computer network and stores data on vetting requests, analyses, and results. Access to the RAM database will require a user identification name and password and approval from the RAM System Owner and ISSO. An audit trail is maintained and periodically reviewed to monitor access to the system. Authorized government personnel and 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.

b. What privacy orientation or training for the system is provided authorized users?

Only cleared and authorized personnel may access the system in their specific roles which are monitored and controlled by the system administrator and the Information System Security Officer (ISSO). Those personnel with access to the Department's OpenNet system must complete annual cyber security awareness training.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

The Department of State maintains all classified records in an authorized security container with access limited to authorized government personnel and authorized contractors.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

No technologies create a privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since no technologies create a greater than normal privacy risk, this category does not pose a privacy threat for RAM.

Risk Analysis and Management (RAM) PIA

12. Security

a. What is the security certification and accreditation (C&A) status of the system?

The RAM system received its Authorization to Operate on 10/19/2012. The system has a FIPS-199 Security Categorization of "Moderate."