

Email the completed PIA to
PIAteam@state.gov

RAM PIA

1. Contact Information

<p>A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services</p>

2. System Information

- (a) Name of system: Risk Analysis and Management (RAM)
- (b) Bureau: Administration
- (c) System acronym: RAM
- (d) iMatrix Asset ID Number: 7233
- (e) Reason for performing PIA:
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): [Click here to enter text.](#)

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 - Yes
 - No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?

RAM's Authority to Operate (ATO) was granted on October 31, 2013. The RAM system has completed its triennial security re-certification and is expected to be reauthorized in November 2016.
- (c) Describe the purpose of the system:

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 utilizes 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 screening 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.
- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

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 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.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 301, 302, Management of the Department of State;
- 22 U.S.C. 2581, General Authority;
- 22 U.S.C. 2651a, Organization of the Department of State; 22 U.S.C. 2677, Availability of Funds for the Department of State;

- 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.; 18 U.S.C. 2339A, 2339B, and 2339C. **Section 531 of the Foreign Assistance Act of 1961.** Also see Executive Orders 13224, and 12947, as well as Homeland Security Presidential Directive- 6.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: State-78, Risk Analysis and Management Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): 12/6/2011

No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number: (DAA-0059-2012-0004)
- Length of time the information is retained in the system:
"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 form will be destroyed after the information has been converted to an electronic medium and verified, when no longer needed for legal or audit purposes.
- Type of information retained in the system:

Information retained in the system will include the name, date, and place of birth, gender, citizenship(s), and government identification numbers, such as U.S. passport or Social Security numbers if U.S. citizen or Legal Permanent Resident, address, telephone numbers, and e-mail address.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes No

- If yes, under what authorization?

22 U.S.C. 2151 et seq.; 22 U.S.C. 2751, et seq.; 22 U.S.C. 2601 et seq.; 18 U.S.C. 2339A, 2339B and 2339C; Executive Orders 13224, 13099, and 12947, as well as Homeland Security Presidential Directive- 6

- Section 7034(e) of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2016 (Div. K, P.L. 114-113)
- Section 531 of the Foreign Assistance Act of 1961
- Section 551 of the FAA
- Section 571 of the FAA
- Section 582 of the FAA
- Sections 620A, 620G, and 620H

(c) How is the information collected?

Information is obtained directly from the organization, entity, or individual. The organization, entity, or individual seeking funding provides 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.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

- If you did not select "Department-owned equipment," please specify.

[Click here to enter text.](#)

(e) What process is used to determine if the information is accurate?

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

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Contractors/Grantees are required to re-submit information for vetting per the schedule established by the requesting program area.

(g) Does the system use information from commercial sources? Is the information publicly available?

RAM analysts review information that is collected from commercial and public databases. The information is available via the internet and through subscriptions.

- (h) Is notice provided to the individual prior to the collection of his or her information?
Notice that information will be collected will be provided when a solicitation is announced. If an individual is seeking funding, that individual will provide the information. Additionally, the DS-4184 has a Privacy Act Statement, and notice is provided by the publication by the publication of STATE-78.
- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No
 - If yes, how do individuals grant consent?
Information is obtained directly from the organization, entity, or individual. 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.
 - If no, why are individuals not allowed to provide consent?
Click here to enter text.
- (j) How did privacy concerns influence the determination of what information would be collected by the system?
The program collects the minimum amount of required information to establish identity and conduct risk assessment.

5. Use of Information

- (a) What is/are the intended use(s) for 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) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes, all information is used to conduct vetting and provide requesting program areas with information to allow consider/do not consider determinations.
- (c) Does the system analyze the information stored in it? Yes No
 - If yes:
 - (1) What types of methods are used to analyze the information?
Click here to enter text.
 - (2) Does the analysis result in new information?
Click here to enter text.
 - (3) Will the new information be placed in the individual's record? Yes No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? Yes No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Information may be shared with DOS regional bureaus, program offices and other government agencies to the extent necessary to complete the screening process. Only personnel with specific roles in support of vetting or vetting related decisions would be provided access to the data.

- (b) What information will be shared?

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.

- (c) What is the purpose for sharing the information?

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.

- (d) The information to be shared is transmitted or disclosed by what methods?

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.

- (e) What safeguards are in place for each internal or external sharing arrangement?

E-mails or paper files that are shared are marked PII and will be shared only on a need-to-know basis.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The PII in RAM is not shared with any external systems. Only pointers to locate derogatory information are shared on a need-to-know basis. The emails sent on a need-to-know basis are marked as 'Privacy/PII' per security guide lines.

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?

Individuals may contact the office or individual that provided the information to RAM to correct erroneous information and request to have updated information submitted to RAM.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

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.

If no, explain why not.

[Click here to enter text.](#)

(c) By what means are individuals notified of the procedures to correct their information?

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.

8. Security Controls

(a) How is the information in the system secured?

Information in the system is secured through access controls, passwords, closed systems, and controlled outputs. In addition, RAM has implemented encryption for data at rest for PII and other sensitive data.

RAM operates on the Department's OpenNet environment and is not integrated with other internal or external systems. User access is limited to authorized A/LM/RAM staff and is controlled via a registration process. RAM user passwords must be at least 12 characters and changed every 60 days. Since the Department implemented Personal Identity Verification (PIV) cards, both the PIV card and password work together to provide another layer of security. RAM users must use their PIV card to access OpenNet and RAM.

RAM includes an automated process to review account access activity, notify users of pending account disablement based on inactivity and, disabling inactive users. RAM accounts are disabled automatically after 60 days of inactivity. RAM Portal accounts are automatically disabled after 90 days of inactivity. This process is run monthly and generates a report that is sent to the RAM system owner and ISSO. As an additional control, user accounts are disabled after three unsuccessful login attempts.

RAM provides account audit information for RAM and RAM Portal account activities including creation, modification, and disabling. As an additional control, user accounts are disabled after three unsuccessful login attempts. Required account audit information is automatically sent to RAM system owner and ISSO on a monthly basis.

Vulnerability assessments are conducted monthly to identify security compliance and potential risks. All software is kept current to mitigate vulnerabilities.

RAM system changes are submitted to RAM management team for internal review and approval. Before system changes are implemented, all approved requests are submitted to the Enterprise ITCCB for final review and approval for addition to the Department's IT baseline.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

RAM system and database administrators are the only users with direct access to the database for the purpose of performing maintenance. A separate PIV card is required for accessing RAM servers, and database user access is limited to authorized A/LM/RAM staff and is controlled via a registration process. Additionally, all access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

RAM separates RAM web portal users from system/application/database administrators. RAM web portal users do not have access to system management functionality. Access to the RAM Portal is restricted to authorized individuals from prospective contractors/grantees that are invited to submit Risk Analysis Information (RAI) information via the portal. RAM Portal account management is performed by cleared Department of State staff in the RAM system.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

To mitigate misuse within the system, a “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 by US government officials.

Login and logout activity are tracked in RAM, as are the addition or removal of roles within the system. Where determined necessary, audit timestamps of User ID and time of update of a record are also captured.

- (d) Explain the privacy training provided to authorized users of the system.

All Department of State employees are required to take the mandatory Cyber Security Awareness course (PS800) and the Privacy course, PA456 Protecting Personally Identifiable Information, delivered by the Foreign Service Institute.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? Yes No

If yes, please explain.

Information on the Portal is masked/obfuscated once saved to make the information unusable to unauthorized users. In addition, RAM has implemented encryption for data at rest for PII and other sensitive data.

- (f) How were the security measures above influenced by the type of information collected?

The control above was put in place due to the nature of the PII collected.

Users would reasonably expect that their information be visible only to the individuals who need access to it, and that influenced the design such that a role-based system would be used to control and limit access to the data.

9. Data Access

- (a) Who has access to data in the system?

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 Open Net system must complete annual cyber security awareness training.

(b) How is access to data in the system determined?

Access to the data and the RAM system is determined by the role of individual staff members.

Only personnel with specific roles in support of vetting or vetting related decisions would be provided access to the data.

(c) Are procedures, controls, or responsibilities regarding access to data in the system documented?

Yes No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

User access is determined by roles designated by the program manager and RAM user administration and report viewer. Users will not have access to all data in the system.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

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).