PRIVACY IMPACT ASSESSMENT

Risk Analysis and Management PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: July 2021
(b) Name of system: Risk Analysis and Management
(c) System acronym: RAM
(d) Bureau: Administration
(e) iMatrix Asset ID Number: 7233
(f) Child systems (if applicable) iMatrix Asset ID Number:
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?

☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)

☒Yes
☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes
☐No

(c) Describe the purpose of the system:

The RAM system provides 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. The information will include records of individuals, organizations or businesses cleared during the vetting process.

(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:

- Name
- Date and place of birth
- Gender
- Citizenship(s)
- Government identification numbers (such as U.S. passport or Social Security numbers, if U.S. citizen or Legal Permanent Resident)
- Address
- Telephone number
- Work 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?

- 22 U.S.C. 2151 et seq., Foreign Assistance Act of 1961;
- 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;
- Homeland Security Presidential Directive- 6;
- Section 7034(e), Sections 620A, 620G, and 620H of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2021 (Div. K, P.L. 116-260) and similar provisions in prior year acts

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

☒Yes, provide:
- SORN Name and Number: Risk Analysis and Management Records, STATE-78
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 6, 2011

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

(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 Office 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 (consolidate as much as possible):
- Schedule number: DAA-0059-2012-0004
- Disposition Authority Number: DAA-0059-2012-0004-002
- Length of time the information is retained in the system: Temporary. "Yea" decisions will be deleted one year after a contract or grant is awarded. "Nay" decisions will be deleted seven years after a final decision. Organizations and businesses applying for Department of State funds submit the DS- 4184 Information Form.
- Type of information retained in the system:
  Information retained in the system will include records of individuals, organizations or businesses cleared during the vetting process, such as: 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) On what other entities above is PII maintained in the system?

☐ Members of the Public

☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

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

☒Yes ☐No ☐N/A

- If yes, under what authorization?

- 18 U.S.C. 2339A, 2339B, 2339C;
- 22 U.S.C. 2151 et seq.; Foreign Assistance Act of 1961;
- Executive Orders 13224, 13099 and 12947;
- Homeland Security Presidential Directive 6; and
- Section 7034(f) of the Department of State, Foreign Operations, and Related Programs Appropriations Act, 2021 (Div. G, P.L. 116-260) and similar provisions in prior year acts.

(d) How is the PII collected?

Information is obtained directly from an 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 electronic submission through a secure portal.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Accuracy of the information provided on the DS-4184 form is the responsibility of the organization, entity, or individual seeking funding. Before submitting the DS-4184 form, the record subjects are presented with a checkbox to certify the accuracy of the information. The PII provided on the DS-4184 is the information that leads RAM to the potential risk information and verification. The information is not checked against any other source of information for accuracy before it is used to make decisions about an individual.

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

Yes, the information is current. The information remains current as it is up to the contractors/grantees to log into the real time application and submit their current information to RAM once every year. Record subjects have an option not to submit their information which would result in them not being considered for the funding. The information is not checked against any other source of information to ensure it is current before it is used to make decisions about an individual.

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

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

(i) How was the minimization of PII in the system considered?

During the requirements analysis phase of the system design, it was determined that the Social Security number, or any other comparable Government ID, is required to perform the risk analysis. As such, RAM program collects the minimum amount of required information to establish identity and conduct risk assessment.

5. Use

(a) What is/are the intended use(s) for the PII?

The Department of State maintains the PII to support the vetting of directors, officers, or non-governmental organization employees who apply to the Department of State for contracts, grants, or other funding. The information collected from 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. There are no collateral uses of the PII outside of the system.

(b) Is the use of the PII 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 PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(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

(d) If the system will use test data, will it include real PII? ☐Yes ☒No ☐N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: Information may be shared within DoS regional bureaus and program offices with high level Department of State officials to the extent necessary to complete the screening process of funding applicants. Specifically, only personnel with specific roles in support of vetting or vetting-related decisions are provided access to the shared data.

External: Limited information may be shared with other Government agencies at the request of those agencies as needed. For example: DOJ.

(b) What information will be shared?

Internal: Information shared includes 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 number, and e-mail address.

External: Information shared includes 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 number, and e-mail address.

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

Internal: The information is shared within DoS regional bureaus and program offices with high level Department of State officials who will make the decision to approve or deny the funding application based on national security risks.

External: PII of record subjects is shared with other government agencies as necessary to meet the national security considerations. 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.

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

Internal: PII will be shared via email on a need-to-know basis.

External: PII will be shared via email on a need-to-know basis.

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

Internal: The shared data are both encrypted as well as in read-only format to ensure the integrity of the data. E-mails that are shared are marked PII and will be shared only on a need-to-know basis.

External: The shared data are both encrypted as well as in read-only format to ensure the integrity of the data.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, the electronic DS-4184 form that is used to obtain this information has the link to an approved Privacy Act statement (PAS) on each page. This PAS provides the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory. It also provides the applicant with information pertaining to the System of Records Notice (SORN), Risk Analysis and Management Records, STATE-78, that governs the collection of this information where the applicant can learn more about how their PII will be utilized.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒Yes ☐No

If yes, how do record subjects grant consent?

Before submitting the DS-4184 form, the record subjects are presented with a checkbox to certify that they understand that the U.S. Government may rely on the information to process their request for funding. Additionally, the form has a button to grant consent and submit the information to RAM for risk analysis. Record subjects have an option not to click the submit button which would result in them not being considered for the funding.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

Once record subjects' application has been submitted, they cannot access their PII within RAM. However, applicants can contact the RAM team to return the submission to make any updates. RAM can be reached at RAM@state.gov. On the interface for RAM, there

are two ways that people are informed of this. The first is through the FAQs. The second is through the help button presented on each page which directs record subjects to contact RAM@state.gov, for any questions concerning grants/contracts, individuals, or submissions.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Once information is entered into the RAM Portal, all PII is masked. On the review and submission page, there is an option provided to preview the information that is being submitted. Record subjects can verify the information and correct inaccurate or erroneous information. Once the application has been submitted, applicants can contact the RAM team to return the submission to make any updates. RAM can be reached at RAM@state.gov.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

If a submission is found to have errors, RAM analysts return the submission and an email is sent to the point of contact (organization or individual) to inform them that the information submitted was incorrect. The office or individual that provided the information is responsible for correcting any misinformation and resubmitting it to RAM.

8. Security Controls

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

The information in RAM is secured by:

1. Encrypting the data at rest.
2. Restricting access to users based on their roles.

RAM implements least privilege roles by grouping related functionality. Access to the data is given based on the roles and privileges.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to RAM and its PII is role-based:

DoS Employees:

- System Owner: Has complete access to the system and all of the PII within it. The system owner can read, update, and delete all PII.

- RAM Users: Have complete access to RAM, except the administrative module used for maintenance of the system, and all of the PII within the system. They can read, update and save all PII.
- Program Officers: They do not have access to any PII. In terms of system access, they can only view the vetting status or results and details related to the program office's specific contracts or grants.
- Country Restricted Users: They do not have access to any PII. They can only view the contracts/grants belonging to their specific country.
- Post/Bureau Restricted Users: They do not have access to any PII. They can only view the contracts/grants belonging to their specific post/bureau.

Contractors:

- System Administrators: Have complete access to the system and all PII within it. They can read the data but can only update and delete the data when requested by system owner and/or RAM users.
- Developers: Do not have access to RAM system via DoS systems (i.e. OpenNet), but do have access within the development environment. They cannot view any of the PII in RAM. They can view test data (which is not real PII).

Portal Users (DMZ):

- Portal Users (record subjects or their representatives, who are grant applicants): Authorized external users or DoS employees who can access RAM's external interface and submit the PII of record subjects to RAM for risk analysis PII is masked at submission and no longer available for review.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Management approval is required for access to this system and the data within it, and approval is based on position as well as need-to-know. Total data access is not granted to all users. Data access is limited according to the role-based restrictions as explained in 8b. Audits are completed every month by the system administrators to remove access to the system of employees who no longer have a need-to-know.

Portal users require a username and password to log in to the public-facing portal. Access to the public-facing portal requires authorization from the system owner and is granted to limited personnel authorized to submit record subjects' PII to RAM for risk analysis. It is mandatory that all users change their password once every two months.

(d) How is access to data in the system determined for each role identified above?

Access is determined on a "need to know" basis. Apart from RAM TEAM Users, system administrators, and the system owner, no other users have access to the PII within RAM.

System Owner: Based on the overarching role and responsibilities to manage the system and PII, the System Owner has complete access to all of the PII within RAM.

RAM TEAM Users: RAM users are responsible for accepting PII and conducting the vetting process and are granted access to RAM by the system owner. They have access to all of the PII within RAM.

System Administrators: System Administrators are approved by the system owner to access all of the PII within RAM. They can read the data, update, and delete data only at the direction of the system owner or RAM TEAM user.

Program Officers: They do not have access to PII.

Country Restricted Users: They do not have access to PII.

Post/Bureau Restricted Users: They do not have access to PII.

Developers: They do not have access to PII. They can view test data (which is not real PII).

Portal Users (record subjects or their representatives, who are grant applicants): External users or DoS employees who can only access the RAM Portal application in external interface using the credentials provided by RAM System do not have access to PII. They are only able to enter PII. All PII is masked at submission.

(e) What monitoring, recording, auditing safeguards, and other controls 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 program managers. 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.

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

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no role-specific training. All Department of State employees are required to take the mandatory Cyber Security Awareness course (PS800), which has a privacy

component. All OpenNet users are also required to take PA318, Protecting Personally Identifiable Information, biennially.