PRIVACY IMPACT ASSESSMENT

myGrants

1. Contact Information

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

2. System Information

(a) 02/22
(b) Name of system: myGrants
(c) System acronym: myGrants
(d) Bureau: A (A/LM/PMP/SYS)
(e) iMatrix Asset ID Number: 253899
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA into new template

(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 myGrants system provides a centralized and integrated solution for federal assistance issued by domestic bureaus and allows Bureaus to carry out specified grants work by assisting in the issuance and monitoring of federal assistance to the award recipients. The

information collected and maintained in this system is necessary to support the end-to-end federal assistance planning, pre-award, award, post-award, and closeout processes for the Department, alongside Integrated Logistics Management System (ILMS). The system integrates with A/LM/PMP/SYS ILMS platforms, PeopleSoft and Ariba for award file storage and award issuance.

The myGrants system is based on the ServiceNow Software as a Service (SaaS) solution hosted within the ServiceNow cloud. The Bureau of Administration, Office of Logistics Management, Program Management (A/LM/PMP) owns the application

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

PII is collected from two groups of individuals:

- DoS Employees/Contractors
- Grantees/Grantors - Recipients of federal financial assistance and those issuing federal financial assistance

The following is the list of PII myGrants collects, uses, maintains, or disseminates from both groups:

- First and Last Name
- Business E-mail Address
- Business Address
- Business Phone Number

From grantees only:

- Employer Identification Number/Tax Identification Number (EIN/TIN)

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

- OMB 2 CFR 200 Omni (Circular Grants Reform)
- Digital Accountability and Transparency Act of 2014, Public Law 113-101
- Federal Grant and Cooperative Agreement Act, Public Law 95-224
- Foreign Assistance Act (22 U.S.C. 2151 et seq.)
- Arms Export Control Act (22 U.S.C. 2751 et seq.)
- Migration and Refugee Assistance Act (22 U.S.C. 2601 et seq.)
- Department of State, Foreign Operations, and Related Programs Appropriations Act (Div. K, Pub. L. 116-260)
- United States Information and Educational Exchange Act of 1948 ((22 U.S.C. 1431 et seq.)
- Mutual Educational and Cultural Exchange Act of 1961 (22 U.S.C. 2451 et seq.)

- Section 1287 of the National Defense Authorization Act for Fiscal Year 2017 (as amended by section 1284 of the National Defense Authorization Act for Fiscal Year 2019)

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

☒Yes, provide:
- SORN Name and Number: Integrated Logistics Management System, State-70
- SORN publication dateFebruary 21, 2006
- An updated version of State-70 is in clearance as of the date of this PIA.

☐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):

- Disposition Authority Number:
  DAA-GRS- 2013-0008- 0007 (GRS1.2, item 010)
- Length of time the information is retained in the system:
  3 years
- Type of information retained in the system:
  Records related to the coordination, implementation, execution, monitoring, and completion of grant and cooperative agreement programs

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?

(d) How is the PII collected?

The information is collected in two different ways. First, the information is collected from end-users when they enter it as part of their initial account set-up procedure on the online Access Request Form in the myGrants system. End-user information such as name, business e-mail address, and business phone number are entered into the end-user profile page by the end-user. The myGrants system help desk personnel can also enter this information on behalf of grantor or grantee end-users when setting up their accounts.

The second way PII is collected is via myGrants electronic forms filled out by prospective grantees as part of the application for federal assistance. The myGrants electronic forms are SF-424 (Application for federal assistance), SF-424A (Budget Information for Non-Construction Programs), SF-424B (Assurances, Non-Construction Programs) and/or SF-LLL (Disclosure of Lobbying Activities). OMB has approved each referenced form.

(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.

The myGrants system is a Software as a Service cloud product hosted in the ServiceNow Cloud data center.

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

Accuracy of the information is the responsibility of the individual end-user who provides their own information on their end-user profile and on the forms they submit. The information can be updated by the end-user if the individual identifies the information to be inaccurate. If the email address changes, the end-user will be responsible for contacting myGrants support desk to request the update. Also, myGrants system administrators perform annual end-user reconciliation and account review to ensure accuracy of PII in the system.

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

The myGrants system administrators are responsible for maintaining information such as end-user account control, ensuring it remains current, and performing annual account reviews to ensure accuracy. End-users are prompted to review their profile and confirm accuracy annually. If changes need to be made the end-user may also update their information such as name, business e-mail address, and business phone number directly on their end-user profile to ensure the information is current and accurate. It is the individual's responsibility to submit the data correction request to the myGrants help desk to implement any email address updates.

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

No, myGrants does not use information from commercial sources nor is the information publicly available.

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

Privacy concerns are at the forefront of the system design and any enhancements made. The myGrants system only collects the minimum amount of PII necessary to support the purpose of the system.

5. Use of information

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

Information is used to support issuance of domestic federal assistance. Name, business e-mail address, and business phone number are necessary to create the end-user profile and required to contact a recipient throughout the lifecycle of the award.

Tax ID is collected on the application form when a grantee end-user applies for a funding opportunity. This Tax ID is used to validate a grantee end-user's identity and to track future payments if their organization is issued federal assistance funding.

(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, information is solely used for issuing federal assistance. No collateral uses exist for the information collected by the system.

(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:
The myGrants system shares federal assistance recipients' information with the program and grants offices issuing the federal assistance within the State Department. Also, myGrants shares information with the Integrated Logistics Management System (ILMS) platforms, PeopleSoft and Ariba, which are also A/LM/PMP/SYS applications.

All 29 State Department domestic bureaus, along with 15 overseas posts (Budapest, Gaborone, Brasilia, Kabul, Cairo, Mission India, Bogota, Mission Pakistan, Guatemala City, Panama City, Ouagadougou, Abuja, Dakar, Santo Domingo, and Tegucigalpa) use myGrants. More overseas posts will begin using myGrants in FY22 and onward, so this scope is subject to increase.

External:
PII in myGrants is not shared externally.

(b) What information will be shared?

Internal:
The sharing of federal assistance recipients' information with program and grants offices issuing the federal assistance within the State Department and ILMS platforms includes:

- First and last name, business address, business phone number, business e-mail address, and vendor/employer/applicant Tax ID.

  End-users will have access to the award records associated with the offices on their profile, and they cannot view awards for other bureaus/offices.

External:
N/A

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

Internal:
Information is shared with the Department's program and grant offices to facilitate issuance of federal assistance awards.

For ILMS platforms, the information is shared for award file storage and award issuance.

External:
N/A

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

Internal:
Internal data sharing with ILMS platforms is transmitted bidirectionally via encrypted batch transfers on the OpenNet network using FIPS 140-2 compliant TLS1.2.

External:
N/A

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

Internal:
Internal sharing with the Department's program and grants offices and ILMS platforms is safeguarded by FIPS 140-2 encryption.

External:
N/A

7. Redress and Notification

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

The PAS is currently on all grants forms that collect PII except one, which will be implemented by beginning of March 2022.
A general privacy notice will also be presented to the end-users as they initially log onto the system and is expected to be rolled out mid-February 2022. This is displayed on their initial log on and requires end-user acknowledgement via a checkbox that they're aware that the system will require them to submit some PII.

(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?

Record subjects grant consent to the use of their information when they 1) submit the requisite portions of their profile on myGrants, or 2) email the information to ILMS Support Help Desk. Failure to provide the required information will result in inability to access the modules to complete their duties.

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

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

End-users can view and update their information on their end-user profile page in myGrants, as well as look up any forms they have submitted in the system by searching by key indicators such as full name, type of requests, etc. It should be noted that all record subjects will have an account in myGrants for the issuance and tracking of federal assistance to the recipients of the award.

Additionally, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-70.

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

☒Yes ☐No

If yes, explain the procedures.

Record subjects update their personal information in their end-user profile in myGrants. They are also able to cancel and re-submit myGrants requests/forms that have inaccurate information. In addition, record subjects can submit a ticket to the ILMS Support help desk to correct any erroneous PII.

If no, explain why not.

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

Grantees are notified on how to correct their information during webinar training, which includes training materials for the respective application modules on processes and procedures to correct wrong inputs/information. In addition, end-users can find information on the procedures to update their PII on the support section which is available within the system.

8. Security Controls

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

The information is secured via multifactor authentication to access the system as well as the implementation of data at rest encryption. Information is accessed over a secure HTTPS connection and secured by using the concept of 'least privilege' which necessitates granting access only needed for the end-user's approved role, as indicated on their account request form. Grantee accounts only have the ability to submit applications and view prior applications that the grantee has already submitted. Additional roles and groups are assigned to grantor account to see the forms only for their office which have been routed to their group. The system complies with all Department security mandates as well as RMF security controls.

The system relies on inherent security controls native to the FEDRAMP-approved GovCommunity Cloud (GCC) on which it resides, as well as the inherent security controls from the cloud-service provider ServiceNow, in addition to the implementation of all Department of State security mandates, applicable NIST 800-53 controls and by conducting annual security assessments. Furthermore, the transfer of this data between systems is encrypted following standard Department of State encryption protocols.

(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).

System Administrators: Administrators have access to PII as part of their system operations and maintenance responsibilities. This role has access to all end-user profile pages and the following PII listed below:

- First and Last Name
- Business E-mail Address
- Business Address
- Business Phone Number
- EIN/TIN

Support Users: Help desk role or functional support permission, designated for Tier 1 and 2 help desk users, as well as Tier 3 system technicians. This role permits access to view and update bureau configurations and end-user accounts. This role has access to all end-user profile data and application data, and to the following PII elements:

- First and Last Name
- Business E-mail Address
- Business Address
- Business Phone Number
- EIN/TIN

Grantors: State Department users that assist grantees with the federal assistance planning, pre-award, award, post-award, and closeout processes. They are permitted to access only on the front-end and are restricted to visible records by the office/business

units they are associated with. This role has access to view the following PII elements from grantees and grantors in the business units they are associated with, except for EIN/TIN which is only from grantees:

- First and Last Name
- Business E-mail Address
- Business Address
- Business Phone Number
- EIN/TIN

Grantees: Individuals applying to and/or recipients of federal assistance grants. These end-users are permitted access only to their own data profile which includes:

- First and Last Name
- Business E-mail Address
- Business Address
- Business Phone Number
- EIN/TIN

(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.

The myGrants system implements a role-based access control (RBAC) process to allow the minimum access to the system and to data for the individual to perform their job function. .

System Administrators only have access to manage end-users and are provided training and the myGrants user administration handbook which provides the information necessary to accurately create and configure end-user accounts. System Administrators perform annual review of accounts to ensure the active accounts are valid end-users and that only approved roles and groups are assigned to the account.

End-users (potential grantees) submit an account request form which is reviewed and approved by their supervisor, as well as the Information System Security Officer (ISSO) prior to granting the account. An annual review of accounts is conducted by supervisors and the ISSO to ensure access is granted at the correct level.

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

For the roles specified in 8(b), access to data in myGrants, and all its modules, is restricted based on the permissions granted by their approved access request form. The access request form is reviewed and approved by the individual's supervisor and help desk personnel. Grantors are required to provide proof of federal assistance training attendance and a state.gov email address to get access. Grantees require grantor approval for their access request form. System administrators and support users also require State.gov accounts and supervisor approval for their access request forms. Access to data for each role listed above is identified by the business process owner. The access is

tied directly to the job function or functions for the role and determine the access assigned and required approval.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

All end-users' actions executed within myGrants are logged in a table and viewable/searchable by system administrators and are tracked by ServiceNow. System administrators are unable to edit these logs and can only view for the purpose of continuous monitoring. The system administrators monitor the logs and get email alerts for any attempts at gaining unauthorized access, unusual activity, and integration errors. There is an established baseline of normal system activities, and the system uses audit logs from ServiceNow to monitor and notify on activities outside of that baseline. Login and logout activity are tracked as are the addition or removal of roles within the system. The ISSO also has access to monitor system administrators' actions executed in the system.

(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 specific role-based training. All Department of State employees are required to take the annual mandatory Cyber Security Awareness course PS800, which contains a privacy module, and the biennial privacy course, PA318 Protecting Personally Identifiable Information, delivered by the Foreign Service Institute.