MyGrants

1. Contact Information

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

2. System Information

(a) Name of system: myGrants

(b) Bureau: A/LM/PMP/SYS

(c) System acronym: myGrants

(d) iMatrix Asset ID Number: 253899

(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):

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?
In progress

(c) Describe the purpose of the system:
The MyGrants system supports the Department's mission requirements for providing a centralized and integrated solution for Federal Assistance issued by domestic bureaus. MyGrants is based on the ServiceNow software as a service (SaaS) solution hosted within the ServiceNow cloud. A/LM/PMP/SYS has configured customized forms within the software to support the specific Federal Assistance types required.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
Name
E-Mail Address

Business Address
Phone Number
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
- 4 FAH-3 H-600 Grants And Other Financial Assistance
- Federal Grant and Cooperative Agreement Act, Public Law 95-224

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

☒Yes, provide:
- SORN Name and Number: Integrated Logistics Management System, State 70
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): An updated version of State-70 including the addition of cloud language has been submitted for review.

☐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 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 (e.g., (XX-587-XX-XXX)): DAA-GRS- 2013-0008- 0007
- 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) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No

No SSNs are in myGrants.

- If yes, under what authorization?

(c) How is the information collected?

The information is entered voluntarily by the user as part of establishing their account in myGrants and applying for any federal assistance opportunities. Information may be entered into the system on behalf of the user by a DOS employee if the user does not have access to the system, in which case a paper submission would be provided to the DOS employee.

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.

myGrants is hosted in the ServiceNow FISMA Moderate datacenter which has FEDRAMP Moderate certification.

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

Each myGrants user is responsible for ensuring their data is accurate on their user profile and in forms they submit. DOS employees submitting forms on behalf of users will have a paper copy or email communication from the user as reference.

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

myGrants System Administrators are responsible for maintaining accounts for users and perform an annual account review to ensure accuracy. Individual users may also update the name, e-mail, and phone number on their myGrants user profile to ensure the information is current.

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

No.

(g) Is notice provided to the individual prior to the collection of his or her information?

Yes. A Privacy Act Statement will appear in myGrants on forms which collect PII.

(h) 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?

Users grant consent by logging into the myGrants application and submitting a form that contains PII that they have entered. A user could further decline to enter PII on a specific form and simply enter "dummy" data, and specify in the comments of the form to contact them directly for any sensitive information they did not provide within the request itself.

- If no, why are individuals not allowed to provide consent?

(i) How did privacy concerns influence the determination of what information would be collected by the system?

The minimum amount of personal data required to support Federal Assistance is included in a myGrants user profile (Name, E-Mail, Phone Number). Additional fields (EIN) only appear on forms which may require that information for issuance of an award.

Name, E-Mail, and Business Phone number are tied to all forms as that standard contact information is required for general correspondence with an individual throughout the life of an award.

5. Use of information

(a) What is/are the intended use(s) for the information?
Information is used to support issuance of domestic federal assistance. Name, email, and phone number are required to contact a recipient throughout the lifecycle of the award.

(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, information is solely used for issuing federal assistance.

(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?

(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Information is shared internally with the program and grants offices issuing the award. These are Department of State employees. There is no data sharing outside of the Department of State.

(b) What information will be shared?

Information submitted on the form is shared with the grantors.

(c) What is the purpose for sharing the information?
Information is shared to allow for the issuance of federal assistance.

(d) The information to be shared is transmitted or disclosed by what methods?
Information is shared via workflow functionality which routes a request through any necessary steps in the award process. This workflow may vary based on request type.

(e) What safeguards are in place for each internal or external sharing arrangement?
Grantors are assigned to groups within myGrants and are only able to see requests routed to their group, for their office.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Access to data in the system will be limited to users within an office and by roles ensuring that only users who need to have access in order to successfully process a federal assistance award can see it.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Users are able to view and update their information on their user profile in myGrants, as well as look up any forms they have submitted in the system.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.
Users are able to update their personal information on their user profile in myGrants.
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
On-site training as well as web-based training materials are available. All users have access to training materials regardless of whether they are on site, or remotely attending. Training materials are shared with users electronically as well as posted to the Knowledge Base within myGrants which all users can access.

8. Security Controls

(a) How is the information in the system secured?
Access to myGrants requires a User ID and Password and is accessed over a secure HTTPS connection. Grantee accounts have only the ability to submit applications and view prior applications that the individual has already submitted. Additional roles and groups are assigned to an account which allows a grantor to see the forms only for their office which have been routed to their group.

(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.

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

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

Actions taken within myGrants are logged and viewable by a Department of State system administrator.

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

All Department of State employees are required to take the mandatory 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.

All data within myGrants is encrypted with FIPS 140-2 compliant algorithms at the storage level. In addition, FAM compliant password complexity is in place for authentication within the system.

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

Security measures were put in place specifically to meet FIMSA Moderate and FedRAMP Moderate requirements.

9. Data Access

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

Department of State employees who have been approved for access by a myGrants System Administrator. Grantee accounts have only the ability to submit applications and view prior applications that the individual has already submitted.

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

Access to data is determined by the groups and roles assigned to an individual's myGrants User ID.

(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.

Access to data in myGrants is restricted based on groups and roles assigned to an individual's myGrants User ID.

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

Users can only see forms that they are authorized to browse based on the roles and groups assigned to their user profiles.