1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: 04/25/2011

(b) Name of system: Grants Database Management System

(c) System acronym: GDMS

(d) IT Asset Baseline (ITAB number): 502

(e) System description (Briefly describe scope, purpose, and major functions):

Grants Database Management System (GDMS) allows users to enter grants data and obtain reports about grant actions. The GDMS is web-based and resides on the Department of State OpenNet. The GDMS was deployed fully in January 2003. Work on this application entails maintenance and enhancements. A/OPE is required to report data from GDMS to USASpending.gov as a part of Federal Funding Accountability and Transparency Act (FFATA).

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable):

2009

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?

The information collected and maintained by the system includes name and street address of individuals who are awarded a grant. This information is entered into the system by the GDMS users, usually transcribed from a grant document.

b. How is the information collected?

The information is entered into the GDMS system by the GDMS users from paper grant reports, which is completed by the Grant Officer.

c. Why is the information collected and maintained?

Information is collected and maintained for reporting and analysis of grant funds.

d. How will the information be checked for accuracy?

The information is checked by the office inputting the grant information into GDMS as well as by GDMS System Administrators.

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

2 CFR part 215. 44 USC part 3501.

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

GDMS is an OpenNet application at ESOC and has the applicable 800-53 security controls in place. Information collected is minimal and necessary to fulfill the purposes of the system.

4. Uses of the Information

a. Describe all uses of the information.

Information collected through GDMS is used for reporting, analysis, and submission to www.usaspending.gov per the Transparency Act. However, name and street address are not sent to USA Spending if the grant is for an individual.

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

The use of summary and detailed reports are used to analyze the data. Aggregate information is produced from the grants data. This data does not generate any new personal information.

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

No commercial information, publicly available information, or information from other Federal agency databases is used in GDMS.

d. Are contractors involved in the uses of the PII?

Yes, contractors maintain the system.

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.

Uses of the information collected in GDMS are limited in scope and do not present a great privacy risk. Commercial information, publicly available information, or information from other Federal agency databases is not used.

5. Retention

a. How long is information retained?

We are required to retain the information for 3 years. If any litigation, claim, or audit is started before the expiration of the 3-year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved and final action taken.

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

No appreciable increase in privacy risk is associated with the passage of time. Information collected is extremely limited in nature and does not pose a threat to the record subject.

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?

The information collected in GDMS is not shared with other internal organizations.

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

The information collected in GDMS is not shared with other internal organizations.

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

There is no privacy risk result as the information collected in GDMS is not shared with other internal organizations.

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?

The grants data is shared with USA Spending. However, for an individual grant, name and street address is not passed over to the USA Spending system. The grants information is posted at www.usaspending.gov as part of the Transparency Act.

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

The grant is exported to a text file per the USA Spending.gov format and submitted to https://ffatadata.usaspending.gov/

Individual name and street address is replaced with the following text: “Removed Per PII”.

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

Risk is mitigated through the removal of PII before submission to USA Spending.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

The official System of Record is Global Financial Management System. STATE-73.

http://www.state.gov/documents/organization/107157.pdf

☐ does NOT contain information covered by the Privacy Act.

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

The publication of the SORN in the Federal Register, and the PIA on the Department webpage provide notice to the individuals prior to the collection of their information.

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

No. If an individual wishes to be considered for a grant, they must submit their 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?

No

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.

The SORN and PIA provide advanced notice to the public regarding how the information in the system will be used.

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 may write to the Director, Office of Information Programs and Services, A/ISS/IPS, SA–2, Department of State, 515 22nd Street, NW, Washington, DC 20522–8100.

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

The privacy risks associated with notification and redress are mitigated by the ability for the individual to correspond with the Office of Information Programs and Services.

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?

. To access the system, users must be an authorized user of the Department of State's unclassified network. Access to GDMS 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 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.

GDMS adheres to NIST 800-53 Security Controls including application level audit logs.

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

All Department of State employees must complete the Cybersecurity Awareness course annually. Department of State employees are also required to take the Departments Privacy Awareness Training (PA 459).

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.

As GDMS is accessed through the Department of State's OpenNet platform, certain access controls are in place to ensure that only authorized individuals are able to logon to the system. Audit logs are kept to track access and maintain security on the system. All employees must complete the Department of State's annual Cybersecurity Awareness course designed to educate them on the risks they incur with the use of the Department's OpenNet. Additionally, all employees who desire access to GDMS must request such from the program manager.

11. Technologies

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

No technologies that employ elevated privacy risks are utilized in GDMS.

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

All technologies used are approved and located at ESOC and adhere to NIST 800-53 Security Controls.

12. Security

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

Authority To Operate (ATO) was granted in May 2008, expiring in May 2011. A new Certification and Accreditation is currently underway.