United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Grantee Compliance Database	
Preparer: Mack Zakikhani	**Office: OMS-ARM-OGD**
Date: 9/1/ 2020	**Phone: 202 564-5291**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

The Grantee Compliance Database/Comply App is a comprehensive database for summarizing a wide range of grant recipient related activities. In addition to providing an overview of award information related to each grantee recipient, this database also stores historical information related to the recipient's training activities, indirect cost rate negotiations, pre-award certifications, post award monitoring plans, as well as on-site review, off-site review, and technical assistance activities. All advanced monitoring activities must be recorded in the system with an attached report to count as part of the Grantee Compliance Assistance Initiative as outlined in EPA Order 5700.6. The database tracks information on planned and actual On-Site Evaluative, off-Site Evaluative and/or On-Site Technical Assistance Visits conducted by each Grants Management and Program Office in the Agency. The primary objective of this

database is to provide accurate information to EPA staff in Headquarters, Regional Program, and Grants Management Offices regarding compliance activities that each Program and Grants Management Office performs or plans to perform during any given calendar year.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

Federal Grant and Cooperative Agreement Act, 31 U.S.C. 6301 *et seq.*; Clean Air Act, 42 U.S.C. 1857 *et seq.*; Federal Water Pollution Control Act, 33 U.S.C. 1254 *et seq.*; Public Health Service Act, 42 U.S.C. 241 *et seq.*; Solid Waste Disposal Act, 42 U.S.C. 6901 *et seq.*; Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. 136 *et seq.*; Safe Drinking Water Act, 42 U.S.C. 300j-1; Toxic Substances Control Act, 15 U.S.C. 2609, Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. 9660.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

An Application Security Certification was approved by the Primary ISO, IMO, and SIO as an alternative to an ATO. This certification is scheduled to expire 8/6/2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Yes. OMB 4040-0004; 4040-0006;

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes. The hybrid architecture of this application leverages EPA's Microsoft SharePoint Online offering and the ASP.NET cluster hosted at EPA's National Computing Center (NCC) located at RTP. The type of Cloud Service Provided is Software as a Service (SsaS)

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The Grantee Compliance Database contains information about grant recipients, including the organization's name, location, DUNS, as well as the name of the point of contact for the organization. The user account information for EPA staff granted access to this system includes name and email address.

2.2 What are the sources of the information and how is the information collected for the system?

Organizational information about the grantee recipient is collected by the application through web services offered by the System for Award Management (SAM.gov) system. User account information for EPA staff granted access to this system, including name and email address, is collected in EPA's Microsoft SharePoint Online from the Microsoft Azure Active Directory Domain Service.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Yes. We use SAM.gov. The information collected supports the purpose of the Office of Grants Debarment Grants Program. The EPA Grants Office collects organizational information that is directly relevant and necessary to reporting about a grant.

2.4 Discuss how accuracy of the data is ensured.

Data from the recipients is assumed to be accurate since it is retrieved from SAM.gov. EPA Grants Specialists and Project Officers verify the accuracy of the data using SAM.gov as the authoritative source for the recipient. Compliance data is assumed to be accurate since it is added by EPA staff directly involved in monitoring these grant programs and validated by staff in OMS/OGD

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Risk EPA staff inadvertently distribute data in the Grantee Compliance Database

Mitigation:

There are appropriate controls in place. ROB is also signed by EPA staff to prevent unauthorised information distribution. Mandatory annual Information Security and Privacy Awareness Training is completed by all Agency staff and contractors.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, the application employs Microsoft SharePoint Online site administration controls. Access requests to the app are managed through SharePoint. Only EPA staff involved in grants management activities are granted access. In the App the different levels of access are assigned roles based on the users responsibilities. These include registered user roles for compliance staff and regular users. Furthermore, in the APP there are different roles that imposes limitations and access for the role assigned to the user.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Microsoft SharePoint Online site management documentation is available from Microsoft and the OMS/EI SharePoint team. The access control information is documented in the User Reference Guide.

3.3 Are there other components with assigned roles and responsibilities within the system?

Assigned roles and responsibilities within the Grantee Compliance database are provided only to EPA personnel. There are no other components within the Grantee Compliance Database with assigned roles and responsibilities

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

Science Application International Corporation (SAIC) contractors have an Agency level contract. Yes, we have applied the GS Schedule and FAR clauses to the contract.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are retained in accordance with EPA's Record Schedule 009 and disposed of under National Archives and Records Administration (NARA) disposal authority NARA Disposal Authority: N1-412-07-33c.

Item c: Electronic data - Superfund site-specific
This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters. NARA Disposal Authority: N1-412-07-

33c; Disposable; Destroy 30 years after grant closeout.
Item d: Electronic data - waste water construction and state revolving fund grants
This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters.
NARA Disposal Authority: N1-412-07-33d; Disposable
Destroy 20 years after grant closeout.
Item e: Electronic data - other than Superfund site-specific, waste water construction, and state revolving fund grants
This item is to be used only by the Office of Administration and Resources Management, Grants Management Division at Headquarters. NARA Disposal Authority: NARA Disposal Authority: N1-412-07-33e; Disposable; Destroy 10 years after grant closeout.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Information may be retained longer than needed.

Mitigation:

The records retention schedule applicable to the Grantee Compliance database is properly followed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. Information is not externally shared.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

N/A

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None. There is no external sharing

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The Grantee Compliance Database maintains an audit trail documenting the actions taken in the system. The Grantee Compliance Database is limited to EPA employees within the Agency's grants community.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The Information Security and Privacy Awareness Training is mandatory each year. The course includes information regarding policies and practices that EPA users should follow. The Privacy Act of 1974 and rules of behavior are also discussed.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of unauthorized access to the system. The system has technical controls and policy based on safeguarding security measure that can be audited. Not ensuring users are being held accountable for compliance with policy regarding access to a system may present a risk.

Mitigation:

Auditing and accountability checks are done periodically to ensure safeguarding of Grant Compliance data. Grantee Compliance is a Microsoft SharePoint Online app that employs SharePoint site administration for user management and audit trails. Users of the system must take the Agency Mandatory Information Security and Privacy Awareness Training.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The EPA Office of Grants and Debarment uses information in the Grantee Compliance Database to track recipient compliance.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes__ No_X_. If yes, what identifier(s) will be used.

(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Although this feature is a carryover from the predecessor system Grantee Compliance Recipients and Activities (GCRA) database and is not a necessity.

The app contains a filter that allows a report created by a user in the system to be retrieved by grantee business organization information. Type of grantee business information include DUNS and Company Name

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

Security controls used to protect data in the Grantee Compliance Database are commensurate with those required for an information system that is not rated as moderate or high for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

Technical Safeguards

- Electronic records are maintained in a secure, password protected electronic system.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a risk that information collected and contained in Grantee Compliance Database could be misused.

Mitigation:

To mitigate any risks with regards to use of information in Grantee Compliance Database. Safeguards controls are in place using an access control list. Access to the Grantee Compliance Database is limited to registered EPA users of the database to complete their work. Grantee Compliance users also are required to complete mandatory annual Agency Information Security and Privacy Awareness Training

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Mitigation:

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Mitigation: