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: Electronic Grants Records System (EGRS)	**System Owner: Michael Osinski**
Preparer: Carlyn Perry	**Office: OMS ARM OGD**
Date: 07/27/20	**Phone: 202 564-5309**
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:

EGRS is a semi-automated records management application, designed to capture data/artifacts/attachments out of IGMS (Source system) in order to file/organize them within the Agency's records management solution (currently, Documentum). The system does also allow for manual adds of artifacts/attachments (ie. Records related to grant actions) to be uploaded by authorized EPA staff for storage and records management outside the automated processes.

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?

The EGRS Application will operate under the IGMS SSP. IGMS ATO expires June 11, 2023

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.

No ICR required

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?

Data is stored within the Agency Enterprise Content Management System (ECMS) environment, which is currently Documentum. No, the data is not stored in the Cloud.

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).

EGRS collects data downstream to IGMS/NGGS as mainly unstructured data types (PDFs, DOCx, XLSx, JPGs, and other attachment formats). The unstructured data would namely be artifacts created by IGMS/NGGS (Funding Recommendations, Grant Award documents, Commitment information, etc) as well as attachments related to grant management activities would be collected by this system. Meta data related each document/artifact/attachment is extremely limited as only the grant number or grant family number (data elements) associated to the action, creation and modification dates for records, and the expiry date for

the record is included.

Names, business email addresses, business phone numbers, and business address information for grantee, EPA project officer, EPA grant specialist may be included within the records, however all records are not 'searchable' as attachment indexes are not created nor are there meta data for these items within EGRS.

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

Grant- related information is collected via the Agency's Grant Management system, IGMS/NGGS. All data are moved into EGRS from IGMS and NGGS.

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

No data are taken from commercial or public available sources.

2.4 Discuss how accuracy of the data is ensured.

EGRS, in effect is middleware, as no data is house within the application. Data is moved from IGMS/NGGS (the source system) and inserted into the Documentum file structure. Accuracy is a measurement of a 1-to-1 ratio (ie. File for file) between Documentum and IGMS/NGGS, to keep the documents in sync.

2.5 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

Risk EPA staff inadvertently distribute data in EGRS.

<u>Mitigation</u>:

There are appropriate controls in place that control access to the read-only grant records. Mandatory annual Information Security and Privacy Awareness Training is completed by the Agency staff and contractors to bring awareness.

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?

EGRS is managed by the system administrator in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in who are responsible for Grants Management. User roles and responsibilities for the EGRS Application is determined by the staff's manager within their organization. User access is based on the roles users are assigned in the system.

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

The Access Control List is documented in the SSP.

EGRS is managed by the system administrator in the Office of Grants and Debarment who assigns roles and responsibilities within the system to users in who are responsible for Grants Management. User roles and responsibilities for the EGRS Application is determined by the staff's manager within their organization. User access is based on the roles users are assigned in the system.

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

Assigned roles and responsibilities with EGRS are provided only to registered EGRS personnel. There are no other components with EGRS 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?

Registered EPA Employee and Contractors will have access to EGRS.

Yes, The appropriate Federal Acquisition Regulation (FAR) clauses is in 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.

The information in the EGRS is 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.

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 Electronic Grants Records System 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 stored by EGRS in Documentum is not normally shared outside the Agency. Grant record information is subject to FOIA requests, as well special request Audits by GAO or IG. There is no system to system sharing of information.

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

If in the rare instance that information is shared -- information would be extracted from Documentum and shared to auditors via email or submitted to the FOIA system.
N/A No Information is shared in EGRS.

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?

No system to system information is shared in EGRS requiring MOUs or ISAs.
N/A No Information is shared in EGRS.

4.4 Does the agreement place limitations on re-dissemination?

N/A No system to system information is shared in EGRS.

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:

No external system to system information is shared in EGRS. Manual sharing of information are by request (FOIA, Audit, etc)

Mitigation:

SOPs for FOIA review and release of information are in place and well established

Audit engagements have non-disclosure agreements of any data shared for review. Audit engagement may have other restrictions, because audit findings do not typically include specific

data from the review (but rolled up results from analysis).

No external Information is shared in EGRS.

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 source systems maintain audit trails documenting the actions that users take in the systems. The source systems are limited to registered EPA employees with assigned roles and responsibilities.

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 required each year. The course includes information regarding policies and practices that EPA users should follow. The Privacy Act of 1974 and Rules of Behaviors are also discussed.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

If a system does not have 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:

The source systems have access controls and audit trails for grants. Users of the systems, as well as users of the EGRS, must take the Information Security and Privacy Awareness Training yearly to maintain access to the system.

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.

EGRS is a semi-automated records management application, designed to capture data/artifacts/attachments out of IGMS and NGGS (Source system) in order to file/organize them within the Agency's records management solution (currently, Documentum).

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.*)

Grant records are assigned very little meta data for searching. Data elements include: grant number, grant family number, file creation date, file modification date, and file expiry date. Information may be retrieved by using the grant number.

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 personal sensitive data in Electronic Grants Record System (EGRS) are commensurate with those required for an information system rated moderate for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4.

Administrative Safeguards

- Paper records are maintained in locked file cabinets.

Technical Safeguards

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

Physical Safeguards

- All records are maintained in secure, access-controlled areas or buildings.

6.4 <u>Privacy Impact Analysis</u>: 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.

<u>Privacy Risk</u>:

There is a risk that information collected from the source systems could be misused.

<u>Mitigation</u>:

To mitigate any risks with regards to use of information in the EGRS. Safeguards controls are in place using an access control list. Access to EGRS is limited to registered EPA users of the EGRS application to complete their work. Access to EGRS application is also limited to data needed to do your job. EGRS users also are required to complete mandatory 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: