

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: OARM Data Mart	
Preparer: Carlyn Perry	Office: OMS/OGD, OMS/OAS
Date: 2/2/2021	Phone: 202-564-5309
Reason for Submittal: New PIA _____ Revised PIA _____ Annual Review <u>X</u> _____ Rescindment _____	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u>	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u>	

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

The Agency needs to be able to track monetary awards for grant and procurement records as well as the status of each associated transaction.

The OARM Data Mart contains current and historical Grant and Contract award records, as well as related financial and other referential data.

Grant-related information is collected via the Integrated Grants Management System (IGMS). Contract related data are collected from the EPA Acquisition System (EAS). Budget-related information for both universes (grants, contracts) is pulled from the COMPASS Data Warehouse (CDW).

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?

Yes, the Data Mart has an SSP. It has been authorized to operate through August 1, 2022.

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?

No, the data are not stored in a 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).

The OARM Data Mart contains current and historical Grant and Contract award records, as well as related financial and other referential data. No collection of data directly from users takes place within the scope of the OARM Data Mart.

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 Integrated Grants Management System (IGMS). Contract-related data are collected from the EPA Acquisition System (EAS). Budget-related information for both universes (grants, contracts) is pulled from the COMPASS Data Warehouse (CDW). All data are ported into the Data Mart via Informatica ETL workflows.

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.

The Data Mart does not ensure data accuracy. That is managed by the source systems (EAS, IGMS, COMPASS)

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 Data Mart System.

Mitigation:

There are appropriate controls in place. 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, each user is designated a user role with the scope of the Data Mart. OARM Data Mart is managed by the system administrator in OAS and OGD who assigns role with the system. Only EIAM-authenticated Agency users can access the system; it is not available to the general public. There are different roles that dictate whether or not a particular user has

read-only or read-write privileges with respect to reports.

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

The Access Control List is documented in the SSP. OARM Data Mart is managed by the system administrator in OAS and OGD who assigns role with the system.

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

Assigned roles and responsibilities with OARM Data Mart are provided only to registered OARM Data Mart personnel. There are no other components within OARM Data Mart 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?

Authorized EIAM-authenticated Agency employees and contractors have access to the Data Mart. 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.

The information in the Data Mart is completely rewritten nightly from the source systems. If Records were 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:

If information was retained it may retain longer than needed.

Mitigation:

If information was retained in the OARM Data Mart the records retention schedule applicable to IGMS and EAS would be followed. The data is rewritten each night and not retained.

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.

Yes. Grants data are submitted from the Data Mart to USASpending via semi-monthly flat file submissions. All federal departments and agencies submit their grants data in similar fashion.

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

All federal departments and agencies are required to submit their grants data to USASpending, using a standardized template that protects privacy information where pertinent.

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?

OGD and OAS work with each office to establish a MOU for internal EPA offices.

4.4 Does the agreement place limitations on re-dissemination?

Yes.

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:

The risk is that Data Mart information might be compromised or made too widely available if sharing is not limited.

Mitigation:

External Access is not available. Information sharing agreements, MOUs, new uses of the information, and registration are controlled processes that limit those that can access the information.

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 grant and procurement information. Users of the systems, as well as users of the Data Mart, must take the Rules of Behavior 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.

The Data Mart provides a querying/reporting mechanism for grants and contracts staff to review pertinent Agency data holdings.

The Office of Grants and Debarment (OGD) and the Office of Acquisition Solutions (OAS) need to be able to track monetary awards for grant and procurement records as well as the status of each associated transaction. Its grants and contracts staff need to constantly review the data for accuracy, timeliness, and completeness.

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.)*

Grants and Contracts are assigned a grant/contract number. Information retrieved use non PII data elements to retrieve grants and contracts records in the Datamart.

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?

Data Mart is not a System of Record and does not have a SORN. No information is retained in the system the data is rewritten each day.

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 from the source systems could be misused.

Mitigation:

To mitigate any risks with regards to use of information in the OARM Datamart. Access to the OARM Datamart is limited to registered EPA users who have completed the 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: