

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: OARM Data Mart

Preparer: Matt Moss/Carlyn Perry

Office: OARM

Date: 07/20/2017/9/21/2017

Phone: 202-564-4115/202 564-5309

Reason for Submittal: New PIA_____ Revised PIA_____ Annual Review__X__ Rescindment_____

This system is in the following life cycle stage(s):

Definition ☐

Development/Acquisition ☐

Implementation ☐


Operation & Maintenance ☒

Rescindment/Decommissioned ☐

Note: 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 of the system:

The OARM Data Mart provides authorized users with a read-only querying and reporting interface for Agency grant- and contract-related data. The information collected is a duplicate copy of IGMS and EAS respectively. 

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the system in question?

Title III of the E-Government Act of 2002, Federal Information Security Management Act (FISMA)

The Privacy Act of 1974, PL 93-579, as amended

The Freedom of Information Act, PL 93-502

The Federal Managers' Financial Integrity Act (FMFIA), PL 97-255

OMB Circular A-130, *Management of Federal Information Resources*

OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, December 2004

OMB Circular A-127, *Financial Management Systems*, July 23, 1993

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

1.2 Has a system security plan been completed for the information system(s) supporting the system?

Yes.

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.

Not applicable.

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.

2.0 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.

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

IGMS, CDW, and legacy ICMS and SPEDI data stored in Oracle and Lotus Notes databases.

2.2 Does the system use information from commercial sources or publicly available data? NO If so, explain why and how this information is used.

Yes. It uses information from the federal System for Award Management (SAM.GOV), to ensure accurate grantee and contractor information.

2.3 Discuss how accuracy of the data is ensured.

The OARM Data Mart brings data over from IGMS, EAS, and CDW for integrated, centralized querying and reporting. Accuracy of the source data can only be ensured by the source systems.

2.4 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Specific risks are inherent in the collection of the data elements from source systems.

Mitigation: Risks are mitigated within source systems, the OARM DataMart simply provides and centralized means of accessing.


Section 3.0 Uses of the Information

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

3.1 Describe how and why the system uses the information.

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

3.2 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.)*

The Data Mart is designed to allow users the ability to retrieve data based on specific vendor, applicant, grant specialist, project officer, etc. Specific individuals are identified by first and/or last name, work mailing address, work Email, work phone. 

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved? System does not retrieve information based on personal identifier.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The OARM Datamart does not have a SORN. The SORN for the IGMS system, which provides source data is EPA-53

- 3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.**

No.

3.6 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information collected and contained in source system could be misused.

Mitigation: To mitigate any privacy risks, with regard to use of information in the DataMart or source systems, access to all systems is limited to registered and authorized users only.

Section 4.0 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.

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

Notice is not provided, because no collection of data directly from users takes place within the scope of the OARM Data Mart.

- 4.2 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?**

No opportunities are available to decline or opt out of providing information to the OARM Data Mart, as it is a read-only system and users do not input information directly into the system.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is no risk related to notice.

Mitigation: Given there is no risk, there is no mitigation required

Section 5.0 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.

- 5.1 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?**

The OARM Data Mart system allows for two levels of access, one allowing for viewing existing reports, and the other for generating new reports. In a general sense, all information being made available is considered to be non-sensitive. All authorized users of the system are able to access all data in the system through existing reports as per rights granted via registration with the Agency's Web Access Management (WAM), and a subset of authorized users are further allowed to create new reports.

- 5.2 Are there other components with assigned roles and responsibilities within the system?**

No.

- 5.3 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?**

Data are accessed internally by Agency staff and approved contractors. The pertinent FAR clauses would be included in the contracts governing their employment and are not maintained by this office.

- 5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?**

Access to the Data Mart is controlled via the Agency's Web Access Management (WAM) portal contingent upon approval by OARM. Users are provided access to one of two Data Mart groups via the WAM portal, through a registration process.

- 5.5 Explain how long and for what reason the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the**

schedule number.

The OARM Data Mart is refreshed daily, and only brings over records that are retained in the source systems on a given day. Source systems are official source and maintain records according to schedules.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No.

5.7 Privacy Impact Analysis: Related to Retention

Privacy Risk: No Risk as source systems maintain retention and Datamart is updated as schedules are implemented.

Mitigation: No risk, no mitigation required.

Section 6.0 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.

6.1 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.

System is accessible to EPA internal users only, and not shared regularly with external users. No agreements

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A

6.3 Does the agreement place limitations on re-dissemination?


N/A

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

No Records of disclosure – information is used within the EPA

6.5 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?

Information sharing agreements, MOUs, new uses of the information are brought before OAM and OGD managers for decision-making and formal authorization. New internal access requests to the system are approved through a formal registration process. 

6.6 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: The risk is that Datamart 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 7.0 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.

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

The information pertains to contracts and grants, and does not pertain to an individual. There is no reason an individual would request access to their information.

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

The information pertains to contracts and grants, and does not pertain to an individual. There is no reason an individual would request access to their information.

7.3 How does the system notify individuals about the procedures for correcting their information?

The information pertains to contracts and grants, and does not pertain to an individual. There is no reason an individual would request access to their information.

7.4 Privacy Impact Analysis

Privacy Risk: *The information pertains to contracts and grants, and does not pertain to an individual. There is no reason an individual would request access to their information.*

Mitigation: No mitigation required.

Section 8.0 Auditing and Accountability

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

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

This is a read only system displaying duplicate information from the source systems, IGMS and EAS, for reporting purposes. The system owners grant users authorized access and maintain an updated access control list that is audited to ensure only active users

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

The Agency provides Mandatory Security Awareness Training annually to employees and contractors topic covered: Understanding Controlled Unclassified information and Personally Identifiable Information, (PII) Understanding and protective measures of CUI and PII.

8.3 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: Information in the system is read only, so there is no risk of users changing information. A user access control list is maintained so that only authorized users can view the data.