United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 1/2020)
(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.*** http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: OARMLAN-OAM	
Preparer: Richard Belles	**Office: OMS/ARM/OAS**
Date: December 7, 2020	**Phone: (202) 564-4339**
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: 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 OARMLAN-OAM provides computer services to OAS employees in the Ronald Reagan Building (RRB) / Research Triangle Park (RTP) / Cincinnati and supports one major application: EPA Acquisition System (EAS). The OARMLAN-OAM allows OAS users access to office automation software, additional applications and Agency-provided services, including Intranet and Internet access. It also supports the OAS's website and the OAS service desk helpdesk application which collects information contained in helpdesk tickets (no sensitive PII is collected).

Note: The EAS application has received its own ATO and a separate PIA will be submitted for this system.

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?

- Executive Order 12072 (Aug. 16, 1978);
- Federal Property and Administrative Services Act of 1949, 40 U.S.C. 121;
- Executive Order 9397 (Nov. 22, 1943). 42 U.S.C. 290dd-1, 290ee-1; 5 U.S.C. 7901;
- Executive Order 12564 (Sept. 15, 1986).
- Office of Federal Procurement Policy Act of 1974, 41 U.S.C. 414.
- Public Law 107-67, Section 630
- Executive Order 9397.5 U.S.C. 1104, 5 U.S.C. 1302, 5 U.S.C. 3301, 5 U.S.C. 3304, 5 U.S.C., 3320, 5 U.S.C. 3327, 5 U.S.C. 3361, and 5 U.S.C. 3393;
- The Telework Enhancement Act of 2010 (December 9, 2010); and
- Public Law 111–292.

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?

A security plan has been completed for the OARMLAN-OAM. There is a valid ATO in place, expiration date 9/5/2022.

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.

The OARMLAN is not covered by the PRA.

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 OARMLAN-OAM is not a cloud-system, it is on-premise.

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).

- Work e-mail
- Work phone number

- LAN User ID
- Name

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

The OARMLAN-OAM GSS collects PII from the EPA's Active directory.

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, OARMLAN does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The OARMLAN-OAM and the OAS service desk relies on the EPA's Active Directory to collect accurate data.

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:

The information is contained on, or is transported over, the OARMLAN-OAM GSS contains PII. Due to the information of names, work phone number, work email address, work location and EPA LAN ID, the potential of a breach could exist. If this information was breached or compromised, it could have a low risk of harm to the individual's professional and personal aspects of life.

Mitigation:

Mitigations to protect Privacy include technical, physical, and administration controls. The users of the information are provided Privacy, Security, and Rules of Behavior training on an annual basis. The Agency has a Chief Information Officer (CIO), Information Security Officer (ISO), and Privacy Officer on staff to assist and monitor in protecting the individual's information. Users of the information are only given access to electronic and paper documents that are needed to complete their duty tasks. In addition, the system is audited, and the logs reviewed.

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, there are 3 levels of access within the OARMLAN: User, Technician, and Manager.

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

The current SOP listed below utilizes Role-Based Access Controls, which are in place by default, Service desk users only have access to the information contained in a ticket they created and cannot access tickets and the associated PII from other users. Service desk technicians and managers have access to all tickets. If technician or manager access is needed to perform job functions, a request ticket is created and assigned to the ISSO who will grant technician or manager roles if approved. Access control is documented in the current SOP.

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

No, there are no other components with assigned roles and responsibilities within the system.

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?

EPA employees and contractors will have access to the data in the OARMLAN GSS. Yes, appropriate FAR clauses are included 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.

Information is retained for the life of the system to enable researching completed tickets in the OAS Service Desk, in accordance with record schedule #0055.

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:

Data is permanently maintained, there could be storage issues in the future.

Mitigation:

The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy. Storage capacity is monitored by the administrators of the OARMLAN-OAM to ensure there is enough storage.

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 shared outside of EPA as part of the normal agency operations.

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

This is not applicable, the OARM LAN GSS does not share with external parties.

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?

This is not applicable, however in the event information sharing agreements are required. MOUs and ISAs (as applicable) will be reviewed by the ISSOs and then signed by EPA for approval. The OARM LAN GSS PII is considered not sensitive.

4.4 Does the agreement place limitations on re-dissemination?

This is not applicable, the OARMLAN GSS does not share information.

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:

Un-intentional transfer of downloaded documentation via hardcopy or softcopy to an external party.

Mitigation:

All EPA employees and contractors are required to attend Information Security and Privacy Awareness and Record Management Training, upon hire and annually thereafter, which includes guidance on the appropriate use of PII. The IT Rules of Behavior, which provide guidance related to proper use of IT resources, must be read and signed. Also, PII maintained by the Service Desk is considered protected and is limited to personnel with the required access.

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 in accordance with stated practices in this PIA (Section 6.1)?

OARMLAN-OAM and the OAS service desk access is limited to authenticated EPA employees with assigned roles and responsibilities in AD. The OAS service desk login presents the users with the mandatory login notice that explains privacy expectations. The information system implements technology to audit for the security, appropriate use, and loss of PII. The system enforces a Role Based Access Control (RBAC) scheme to ensure that only the personnel required to view or use the information stored on the system have access. The Information System is configured to set access permissions and audit critical directories and files. The information is configured to bind the identity of the information producer with the information. The system is configured to provide the means for authorized individuals to determine the identity of the producer of the information. Through adherence to Agency privacy policies and implementation of NIST privacy controls ensures the agency uses to stored personally identifiable information (PII) internally only for the authorized purpose(s).

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:

Improper or infrequent audit log reviews may not detect the exfiltration or misuse of PII.

Mitigation:

System audit logs are maintained and reviewed in accordance with EPA CIO AU procedure.

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.

EPA user information is used to identify who creates, modifies, owns and has access to tickets in the OAS service desk.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_x__ No___. 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 primary function of OARM LAN OAM is to provide support to the OAS's website and the OAS service desk helpdesk application which collects information contained in helpdesk tickets (no sensitive PII is collected). Service desk users only have access to the information contained in a ticket they created and cannot access tickets and the associated PII from other users. Information can be retrieved using the name of the EPA employee or LAN User ID through the lookup or search feature in Active Directory by an admin.

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?

System personnel have reviewed the privacy information contained (Work e-mail, Work phone number, LAN User ID, Name) and method of collection (Active Directory) to determine the effect of privacy on individuals. To mitigate these concerns, PII collected has been limited to only that which is necessary to aid in account management duties. Users with access to privacy information have been limited to helpdesk support personnel and information is retrieved in response to request for assistance from system users. In addition, helpdesk personnel are EPA employees and contractors and receive Information Security and Privacy Awareness training (ISPAT) within 30 days of hire and annually thereafter. The OARMLAN is configured to audit user activity and leverages EPA enterprise intrusion detection solutions to protect privacy information.

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:

Access to the OAS service desk is limited to authenticated and registered EPA users who have completed the Rules and Behavior and annual cybersecurity awareness and privacy 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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

PII is obtained using information collected from Active Directory. OARMLAN users are not provided with the opportunity to decline to provide information or opt out of the collection or sharing of their information. However, users are provided with accounts only at their request. If users do not want to leverage the OARMLAN capabilities, they do not have to submit an account request. In addition, EPA provides notice prior to obtaining information for use within the agency active directory system, which is used by the OARMLAN system for account management. In addition, all EPA users view the agency mandated warning banner prior to system login.

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:

OARMLAN users are not provided with notice prior to their information being collected.

Mitigation:

EPA provides notice prior to obtaining information for use within the agency active directory system, which is used by the OARMLAN system for account management. In addition, OMS/ARM/OAS will be updating the warning banner, which must be accepted prior to login to include an updated system-specific privacy notice.

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

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:

None, the OARMLAN do have established procedures to provide redress.

Mitigation:

N/A