

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: ORD Enterprise General Support System (GSS)	
Preparer: Caroline Parton	Office: Office of Research and Development
Date: 5/5/2020	Phone: 919-541-3067
Reason for Submittal: New PIA_____ Revised PIA_____ Annual Review_X___ 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 ORD Enterprise GSS, also known as the ORD LAN, is an EPA General Support System. The ORD Enterprise General Support System (GSS) is a set of systems that provides services and functionality to the ORD scientific community at 13 different United States (US) location in support of the ORD Mission. These IT services and functionality include data transport, scientific workstation computing, specialized analytical laboratory equipment, file and print, database, storage capacity, intranet web services, general IT services in support of scientific research and development, data management, and analysis.

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?

This system does not collect PII, it stores PII collected under these federal authorities Resource Conservation and Recovery Act, 42 U.S.C.6981; Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. 9660; Clean Air Act, 42 U.S.C. 7403; Safe Drinking Water Act, 42 U.S.C. 300j-1; Federal Water Pollution Control Act, 33 U.S.C. 1254; Toxic Substances Control Act, 15 U.S.C. 2609; Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. 136r. Federal Grant and Cooperative Agreement Act, 31 U.S.C.6301 et seq.; Public Health Service Act, 42 U.S.C. 241 et seq.; Solid Waste Disposal Act, 42 U.S.C. 6901 et seq.; Comprehensive Environmental Response, Compensation, and Liability Act, 42 U.S.C. 9660. Other laws may be relevant as well.

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, a system security plan has been completed for the information system supporting scientific research efforts/data collections covered under SORN 34 and SORN 36. The current ATO expires in August 2020.

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 is 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?

The ORD Enterprise GSS is not a cloud system.

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 use, dissemination, and maintenance of the PII data elements/information collected is managed and completed by ORD scientist for specific research efforts. These research efforts are covered under SORN 34 and 36. PII elements are identified under each individual research study or effort covered by these SORNs. PII data elements (medical, name, SSN, DOB, Contact Info, address, and telephone number) are not collected by the ORD Ent. GSS, but can be stored on servers or desktops covered by the ORD GSS SSP.

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

The ORD Enterprise GSS System SSP does not identify each study, these studies are tracked by the ORD research organization and researcher collecting the research data. The collection of this data is not completed through a specific application but is typically provided to ORD scientist in a data file. These data files are stored on servers and desktops covered under the ORD Enterprise GSS SSP.

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. The ORD Enterprise GSS does not use this information, the system takes no action on the information. The system is used to store the information in electronic data files.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data is ensured through and by ORD Quality Assurance Project Plan (QAPP) and Quality Assurance (QA) /Quality Control (QC) processes; researchers are responsible for each research effort and the data collected. The ORD Enterprise GSS is only utilized to store the information collected. ORD Enterprise GSS IT components/systems reside on the EPA Intranet, and are not publicly available or accessible from the Internet

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 risks associated with unauthorized access to this information on stored on ORD Enterprise GSS servers and desktops is addressed through the through the application of the Risk Management Framework (RMF) SP 800-39.

Mitigation:

Implementing the Risk Management Framework (RMF) SP 800-39 which includes categorization of the system via FIPS 199 and selection of NIST 800-53 control set, implementing the required controls, assessing the system annually, authorizing and monitoring the system.

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?

Users authenticate to ORD desktops and servers using Active Directory (user id/Passwords). Designated system administrators and scientists are granted access to their files/folders on a need to know basis and credentials through the agency enterprise AD system by role. AD is utilized to control access to the ORD File server shares and desktops where this information is stored. Enterprise GSS systems reside on the Intranet and are not publicly available or accessible from the Internet.

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

Access Controls are identified within the US EPA Active Directory Administrator's Guide and EPA Information Security – Access Control Procedure CIO 2150-P-01.2.

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

The rights for each user are assigned through Active Directory (user/admin). The Enterprise GSS systems reside on the Intranet and are not publicly available or accessible from the Internet.

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?

Only the individuals selected to participate and oversee the research effort/study will have access to the study data/information. If there are contractors in the research studies, OMS has FAR Clauses included in each 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.

SORN 36 RCS EPA 1004, and the Record Control schedule for SORN 34 is RCS EPA 0566.

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:

The ORD Principal Investigator (PI) may not follow the EPA Records Controls schedule or Federal Acquisition Regulation (FAR) requirements.

Mitigation:

The ORD PI takes annual Records Management and Information and Security Awareness Training. ORD Records and Privacy Liaison Officers are available to assist PIs as needed to understand the requirements.

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.

Each research study is conducted and managed by the researcher. PII is not shared, however the results of the analysis may be. The Enterprise GSS systems reside on the Intranet and are not publicly available, are not accessible via the Internet, and only store the information collected by the researcher.

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

Each research study is conducted and managed by the researcher. PII is not shared, however the results of the analysis may be. The Enterprise GSS systems reside on the Intranet and are not publicly available, are not accessible from the Internet, and only store the information collected by the researcher. The ORD Enterprise GSS does not share this information. See SORNs 34 and 36 for detail.

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?

Not Applicable

4.4 Does the agreement place limitations on re-dissemination?

Not Applicable

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. The ORD Enterprise GSS systems do not share information.

Mitigation:

None. The ORD Enterprise GSS systems do not share 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 information is stored in ORD Enterprise GSS systems on the intranet and only people within the agency have access to their research data.

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

All EPA staff take the Annual Information Security and Privacy training. Those who use privacy related data are trained by the LPO annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Individuals are not trained properly on privacy accountability.

Mitigation:

Annual Information Security and Privacy training is required to be completed by all staff, staff not completing the training are locked out of the network.

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 system does not use the information. The information is stored on the ORD managed system: desktop hard drives and file servers. Enterprise GSS reside on the Intranet and are not publicly available or accessible from the Internet.

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.)

The ORD Ent. GSS (system) does not retrieve information. The information is collected manually by the ORD researcher and stored in electronic data files on ORD Ent. GSS servers and desktops.

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?

SORN 34 and 36 apply to specific ORD research efforts that collect and utilize PII, the information collected is stored on a ORD Enterprise GSS desktops and servers. SORN 34 and 36 do not apply to the entire ORD Enterprise GSS but to collection efforts by the researcher. The data collected by the researcher is then stored on ORD enterprise GSS systems. The ORD Enterprise GSS system permits electronic storage of PII data, but do not conduct electronic searches, queries, or analysis. Analysis of flat data files (i.e. excel) is conducted by the researcher using scientific tools or queries (i.e. R statistical software on a desktop).

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:

1. Unauthorized access.
2. Data Loss.

Mitigation:

1. Active Directory / Access controls on desktops, servers, file shares. The ORD Enterprise GSS systems resides on the Intranet and the data is not publicly available, or accessible via the Internet
2. Individuals are responsible for backing up the data to the ORD Net MyDocs if the data is placed /used on a desktop. ORD File Server shares are backed up via enterprise backup methods, unless explicitly excepted from this process.

***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: