



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 Management Information System (OMIS)	System Owner: Carla Adkins
Preparer: Carla Adkins	Office: ORD/OSIM/AIMD
Date: 9/30/2021	Phone: 513-569-7759
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:

OMIS tracks a wide variety of data, which provides ORD with the administrative tool to support the EPA's environmental mission:

- Budgets and expenses
- Research tasks and outputs
- Extramural vehicles
- Human resources

The records that are relevant to the Privacy Act are those describing personnel and their personnel actions.

These records contain employee details such as name, workforce employee ID, employee type, appointment type, organization, office location, office phone number, office e-mail address, and employer. They may include an emergency contact person and phone number. For Federal and PHSCO employees, the data may include job series and title, grade and step, salary, pay plan, retirement type, service computational date, separation date, personnel actions, and highest educational degree. There are also flags to indicate those Federal employees who are Supervisors, Principal Investigators, Extramural Managers, those who have gone through the Technical Qualifications Board (TQB), and those on the Health & Safety Medical Monitoring Program.

Categories of persons being covered in OMIS are any employee currently or formerly working on the premises of an ORD facility, whether full-time or part-time, such as: Current and former EPA employees; Public Health Service Commissioned Officers (PHSCO) assigned to EPA; employees of other Agencies assigned to EPA under an Interagency Agreement (IGA) or Intergovernmental Personnel Act (IPA); onsite ORD contractors; post-doctorial, pre-doctorial, and summer students; holders of fellowships and internships, NRC research associates, and visiting scientists; students participating in programs such as Student Volunteers, Student Career Experience Program, Student Services Contract Authority, and the McNair Scholar Program; term appointments, temporary hires, and those employed under the Senior Environmental Enrollee Program.

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?

5 U.S.C. 5101 et seq.; 5 U.S.C. 5501 et seq.; 5 U.S.C. 5525 et seq.; 5 U.S.C. 5701 et seq.; 5 U.S.C. 6301 et seq.; 31 U.S.C. 3512; Executive Order 9397 (Nov. 22, 1943); 5 U.S.C. 6362; 5 U.S.C. 6311.

The HR data in OMIS originates in the Agency People Plus System. ORD-related data is received from People Plus.

There is an ISA/MOU in place for Compass Data Warehouse.

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?

ORD has completed a system security plan for OMIS. OCFO is responsible for the security plan for Compass Data Warehouse and People Plus. Yes, the ATO expires 11/2022.

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

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).

First Name, Surname, and Last Name are contained in the OMIS database.

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

Data is downloaded from People Plus and Compass Data Warehouse

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

2.4 Discuss how accuracy of the data is ensured.

People Plus and Compass Data Warehouse ensure accuracy of 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:

Low risk. The information in Compass Data Warehouse and People Plus are checked regularly. This is the same information in OMIS.

Mitigation:

Annual OMIS Security Assessment makes sure that all data is correct. If not, it is corrected.

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. Users are only able to see data base on a need to know basis per job responsibilities.

For OMIS HR, privileges are limited to an individual's own division by default. Basic roles that can be granted include VIEW, VIEW SALARY, and MODIFY, with the MODIFY role being sub-divided into EPA/Federal-type HR records, EPA/non-Federal HR records (e.g., Contractors, Cooperators, and Other type records), and both EPA/Federal and non-EPA/non-Federal records. Users can be given access to OMIS HR records for other divisions via the OTHER VIEW and OTHER MODIFY roles; approval for this access must be approved by the OMIS representatives for all applicable Labs/Centers/Offices. Finally, there are VIEW ALL and MODIFY ALL roles, which grant access to all OMIS HR data; these roles must be approved by the OMIS system owner.

IRMS includes a number of roles to provide access to different functionality and features within the system; additional access controls also allow access to be controlled for different budget levels . For all roles, access is configured for each user at multiple levels: NPM provides access to all ORD data, RC grants access to one or more Labs/Centers/Offices, and Div grants access to specified divisions within a Lab/Center/Office. Different approvals are required depending on the level of access required, and users can hold multiple independent roles (i.e., having VIEW access to one division and ENTRY access to another).

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

Access controls are documented in the OMIS3 Operations & Maintenance (O&M) Manual, Section 4.1.1.2.1: OMIS Privileges. Operational instructions for creating OMIS accounts, granting access, and obtaining necessary approvals are documented in this manual as well.

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

No

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 ORD personnel and EPA ORD contractors. Only people in these two groups that need the information have access to it. Yes, the contractors have the clause in place 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.

OMIS does not have an archive process. The Records Control Schedule is 0467. The records are held for 7 years after the date of closure. That's the records retention schedule for OMIS and this was followed as per ORD RLO.

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:

Low risk, of keeping information longer than needed.

Mitigation:

When record retention is checked regularly, all closed data after 7 years is deleted.

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

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

Not applicable.

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 for external agency sharing. OMIS has an internal MOU/ISA with Office of Chief Financial Officer (OCFO) for Compass Data Warehouse.

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:

Low privacy risk, as information is not shared with any outside entities.

Mitigation:

As the information is not shared with outside entities, mitigation is achieved.

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?

We follow the process and data helps the Office of Resource Management to help ORD'd mission. Only people who need access related to the job have access. There is a annual external audit which ensure data are accounted for and are used for the purpose of collection.

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

OMIS users are covered under the Agency's annual information security and privacy awareness training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of untimely audit to detect any discrepancies in the system.

Mitigation:

Any discovered discrepancy is corrected during annual OMIS assessment.

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.

OMIS tracks a wide variety of data, which provides ORD with the administrative tool to support the EPA's environmental mission:

- Budgets and expenses
- Research tasks and outputs
- Extramural vehicles
- Human resources

The records that are relevant to the Privacy Act are those describing personnel and their personnel actions. These records contain employee details such as name, workforce employee ID, employee type, appointment type, organization, office location, office phone number, office e-mail address, and employer. They may include an emergency contact person and phone number. For Federal and PHSCO employees, the data may include job series and title, grade and step, salary, pay plan, retirement type, service computational date, separation date, personnel actions, and highest educational degree. There are also flags to indicate those Federal employees who are Supervisors, Principal Investigators, Extramural Managers, those who have gone through the Technical Qualifications Board (TQB), and those on the Health & Safety Medical Monitoring Program.

Categories of persons being covered in OMIS are any employee currently or formerly working on the premises of an ORD facility, whether full-time or part-time, such as: Current and former EPA employees; Public Health Service Commissioned Officers (PHSCO) assigned to EPA; employees of other Agencies assigned to EPA under an Interagency Agreement (IGA) or Intergovernmental Personnel Act (IPA); onsite ORD contractors; post-doctorial, pre-doctorial, and summer students; holders of fellowships and internships, NRC research associates, and visiting scientists; students participating in programs such as Student Volunteers, Student Career Experience Program, Student Services Contract Authority, and the McNair Scholar Program; term appointments, temporary hires, and those employed under the Senior Environmental Enrollee Program.

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.)*

Employee ID

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 integrity is constantly checked and maintained.

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:

Low risk misuse. As data integrity is checked regularly.

Mitigation:

Any and every data integrity issue is corrected immediately when found.

***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?

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:

Mitigation: