United States Environmental Protection Agency

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: CINCI/OARM LAN	
Preparer: Helen Lewis	**Office: OARM IRMD CIN**
Date: 5/6/2020	**Phone: 513-569-7712**
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:

CINC/OARM LAN General Support System is the Metropolitan Area Network that provides Agency network access to all users in the Cincinnati Offices of the EPA. This GSS contains servers, printers and some PCs for the OARM immediate office, the Information Resources Management Division (IRMD-CIN), the Human Resources Shared Service Center (HRSSC-CIN), the Facilities Management and Services Division (FMSD-CIN), the Office of Water - Technical Support Center, Office of the Chief Financial Officer – Cincinnati Finance Center (OCFO-CFC), the Office of Acquisition Solutions – Cincinnati Acquisition Division (OAS-CAD), the Office of Inspector General (OIG), and the Office of General Council (OGC), the

Environmental Response Team (OLEM-ERT-CIN), and the Consequence Management Advisory Division (OLEM-CMAD-CIN). It also contains all network Cisco switches in six locations in the metropolitan area.

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?

The information is retrieved from the following source systems:

EZ Hire– **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; Executive Order 9397 (Nov. 22, 1943).

FPPS - EXIM Bank is authorized to request this information pursuant to the following: The Export-Import Bank Act of 1945, as amended (12 U.S.C. 635 *et seq.*); 5 U.S.C. 5101, *et seq.*, 5501 *et seq.*, 5525 *et seq.*, and 6301 *et seq.;* 31 U.S.C. 3512; Executive Order 9397 as amended by Executive Order 13478, relating to Federal agency use of Social Security numbers. 31 U.S.C. 3512 *et seq.;* and 5 CFR part 293.

FED Navigator - Information maintained in FHR Navigator is collected, maintained, and disseminated pursuant to the Federal Trade Commission Act, 15 U.S.C. §§ 41 et seq.

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, ATO expires on 8/2/2021

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).

CINC/OARM LAN General Support System temporarily save names, addresses, DOB, and SSN. This information is saved to the personal network drive of federal employees who is responsible for handling sensitive information and following the Information Directive Procedure while working in the HRSSC.

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

The sources are as followed:

Fed Navigator – process retirement calculations

FPPS – Process personnel actions

EZ Hire (Monster) - Process application supply file – resume intake

The information is retrieved from the source systems and housed on the personal network until the work is complete and then deleted. The information is retrieved by Social Security Number, Name, or Date of Birth

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.

Data is downloaded and it is the source responsibility to ensure adequacy of data

2.5 <u>Privacy Impact Analysis</u>: 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:

Keeping SPII past 90 days

Not properly Encrypting information

Mitigation:

Auditing the systems, reviewing audit logs and providing SPII training.

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, access control levels are based on Roles and Responsibilities.
Typically Read and Read/Write (Modify) for shared files. Typically, users have FULL access by default for files in their home directory. Admins have FULL control of the server and the file system

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

LAN Operating procedures this information can be found in CHAPTER 2 ACCOUNT CREATION, & MAINTENANCE

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?

Federal and Non-Federal Network Administrators rules and behavior and security training.

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.

Media neutral - This schedule authorizes the disposition of the record copy in any media

(media neutral). However, if the format (e.g., electronic) of permanent records is specified in a records schedule approved by NARA, the records are to be transferred to the National Archives in accordance with NARA standards at the time of transfer. If the record copy is created in electronic format or digitized (e.g., imaged) and maintained electronically (e.g., Data on Aquatic Resources Tracking for Effective Regulation (DARTER) maintained in the Office of Water), the electronic records must be retrievable and usable for as long as needed to conduct Agency business and to meet NARA-approved disposition to comply with 36 CFR Sections 1236.10, 1236.12, 1236.14, and 1236.20. Retention and disposition requirements for the various components of electronic systems (e.g., software, input, output, system documentation) are covered in schedule 1012, Information and Technology Management.

Yes, this system does have a control number in which the control numbers is 0553.

Records control schedule GSS schedule

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:

Retaining documents longer than needed

Mitigation:

The record schedule is properly followed

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.

Information is not shared outside of the agency. Except in accordance with the routine uses

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

It’s the responsibly of the source system

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?

The source systems have agreements in place

4.4 Does the agreement place limitations on re-dissemination?

No agreements in place

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:

All sharing agreements have been addressed with the source systems

Mitigation:

None

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?

Follow the Information Directive Procedure

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

Provide Information Security Awareness Training, Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) training annually by the Local ISSO.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

If they modify the data with updating the paperwork

Mitigation:

Make sure that paperwork is updated for the GSS

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.

Used to process HR information and payroll, retirement benefits

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 system is not designed to retrieve information, all of the information is retrieved from the source system which have their own PIA and/or SORN as applicable. Which does not affect the LAN.

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?

OARM-CIN Information Systems Security Officer (ISSO) will adhere to the SPII Documentation Log Procedure (SOP). The ISSO's will perform a monthly scan of the Human Resources Shared Service Center (HRSSC)-CIN users personal network drives, shared drives and secure shared drives to ensure that all such SPII has been erased, returned or destroyed within 90 days. HRSSC-CIN files are purged every days and an email notification is sent to ISSO along with a copy of the artifact.

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

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:

Improper use of information

Mitigation:

Audit logs are reviewed to ensure proper use of information

*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: