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: Great Lakes National Program Office GLNPO.NET	
Preparer: Barry Manne	**Office:** Region 5/GLNPO
Date: 01/04/2021	**Phone:** (312) 353-8015
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 purpose of GLNPO NET is to provide a development/production Internet site available for web projects that are binational or regional in scope without putting US EPA's production network at risk. Separate areas for testing, development, and production are maintained with appropriate user permission levels. The system supports developers from US EPA's Great Lakes National Program Office (GLNPO), US EPA Region 5, state and Environment Canada staff and contractors, as well as US EPA grantees and co-operators. GLNPO.NET is the external commercial namespace, and the network is a typical forest root Microsoft infrastructure.

GLNPO's external network came into being as a result of a Memorandum of Understanding (MOU) between GLNPO and US EPA. The primary stipulation of the MOU is that the two networks, GLNPO.NET and EPA.GOV, would never be connected for any reason. Such a connection would provide a "back door" into

EPA's production network and thereby circumvent the Agency's network security defences. An external network for GLNPO was deemed appropriate due to GLNPO's role of supporting and coordinating external Great Lakes Basin activities and research in collaboration with scientists and researchers external to EPA.

GLNPO NET is designed to house a collection of the EPA's applications and systems for the exchange of unclassified data among U.S. interagency and international partners. It is primarily hosted in a VMware environment located within the Amazon Web Services (AWS) cloud with supporting infrastructure at EPA's Region 5 data center. The on-premises components are physically separated from EPA's operational network to protect it from possible intrusion while still facilitating U.S. interagency and international partner usage. All of the applications and systems within GLNPO NET are specifically intended to facilitate collaboration among international representatives on topics associated with the Great Lakes Water Quality Agreement with Environment Canada and the President's Great Lakes Restoration Initiative. These applications and systems use standard Internet and computing technologies available worldwide to ensure equal access to all and to provide a single access point to community activities and best practices. The applications and systems are not accessible by the general public and do not use or store PII. However, in order to access the applications, users must register via a web form that requests their name, email address, organization, and the application/project that they require access to. The form sends an email to the Account Manager. He or she reviews and approves the request, creates the account in Windows Active Directory, and assigns the account to the security groups that provide the necessary access to program information.

While each GLNPO NET application and/or system will evolve to meet its users' requirements, it provides a subset of the following collaborative tools:

- Interactive Document Archive
- Interactive Calendar for Upcoming Community Activities
- Collaboration Workspace
- Initiatives Research Tool
- Training Center

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?

- Public Law 111-88, October 30, 2009 / Interior Department and Further Continuing Appropriations, Fiscal Year 2010
- 33 U.S. Code Section 1268 – Great Lakes
- Executive Order 13340 – Establishment of Great Lakes Interagency Task Force and Promotion of a Regional Collaboration of National Significance for the Great Lakes May 18, 2004.

Individuals enter relevant First Name, Last Name, Organization, and Email Address into the Great Lakes National Program Office GLNPO.NET application.

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, the system has an SSP in XACTA. The system has been issued an ATO through 1/6/2023.

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?

Yes, most GLNPO NET systems use an IaaS offering provided by VMware Cloud and hosted on Amazon Web Services (AWS) GovCloud. A Virtual Private Network (VPN) connects this environment to a few GLNPO NET systems hosted at EPA's Region 5 data center in Chicago, Illinois. VMware Cloud on AWS GovCloud is in the process of obtaining Federal Risk and Authorization Management Program (FedRAMP) Authorization and has achieved the FedRAMP Ready High designation with the Joint Authorization Board (JAB) consisting of representatives from the Department of Defense (DoD), Department of Homeland Security (DHS) and General Services Administration (GSA). The components that are hosted at EPA's Region 5 data center are located on a network that is physically separated from EPA's operational network.

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 system collects, processes, and stores First Name, Last Name, Organization, and Email Address for the purposes of user registration and application login only.

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

The information is self-reported by individuals applying for access to the system.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

All collected PII is self-reported by individuals. The confirmation of the accuracy, relevance, timeliness, and completeness of this PII is limited to ensuring all required fields are completed and valid email address syntax is used through automated validation included with the online forms.

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 (minimal) to none. The data is self-reported by users directly and human error can lead to inaccurate entry.

Mitigation:

If any data is inaccurate, the account manager can update the date to correct the information.

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, the system has various control levels to prevent users from accessing data outside of that necessary to perform their job functions. GLNPO.NET access controls are enforced with access control lists via Microsoft Active Directory user access configurations. Only Active Directory Domain Administrators can access user account information.

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

GLNPO.NET Access controls are documented within the AC family of security controls of the System Security Plan. The GLNPO.NET Account Manager authorizes user access and group/role membership within Microsoft Active Directory and other system components. The

GLNPO.NET ISSO authorizes Domain Administrator level access, which is the only role with access to user account information.

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

GLNPO. NET includes a division of duties and functions by role.

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 have access to the data/information in the system. Yes, the FAR clauses are included.

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.

GLNPO.NET's records are retained indefinitely, and accounts are disabled rather than deleted. The system falls under EPA Records Control Schedule 0090.

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:

Unauthorized individuals gaining access to PII.

Mitigation:

- Employ the least privilege principles to data access.
- Review Audit logs to ensure data is not intentionally deleted or altered.
- Rules of Behavior acknowledgment and Security Awareness training are required for key roles.

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 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.

Not applicable. GLNPO does not share PII data externally.

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. GLNPO does not share PII data externally.

4.4 Does the agreement place limitations on re-dissemination?

N/A

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:

There's no risk. GLNPO does not share PII data externally.

Mitigation:

N/A.

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?

GLNPO.NET' system audit logs are enabled for accountability. The ISSO ensures security controls corresponding to the privacy security requirements defined in NIST Special Publication (SP) 800-53, including control enhancements, are tested, reviewed, and assessed annually.

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

EPA personnel complete an Information Security and Privacy Awareness and General Privacy Awareness Training course on an annual basis. The training course instructs personnel not to disseminate PII information to unauthorized individuals and how to secure information using approved techniques such as encryption. During these trainings, personnel are instructed not to release agency data classified as PII/PA/CUI to unauthorized users. An action to enforce such behavior is provided in the National Rules of Behavior. Failure to comply could result in the removal of system access. Unauthorized disclosure of EPA sensitive information, including PII, may result in legal liability for the offender.

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. Data is encrypted while in transit and at rest.

Furthermore, account restrictions and controls exist within the system. For privileged account users, these controls exist:

- Authenticator/Password Management – Logs and timed password change requirements
- Account Management – Need-to-know access; login failure logs
- Access Enforcement – Application and monitoring of access privileges
- Least Privilege – Minimum tools required for a user to perform his/her function
- Unsuccessful Login Attempts – Audit log reviews on periodic basis

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.

GLNPO.NET uses the information to create an account and issue access to the required application/project.

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 scientific data housed within GLNPO.NET is retrieved by users in various ways depending on the application being used. Examples include the location where the data was collected, the type of data needed, or a specific scientific study, etc. However, the data is never retrieved using a personal identifier.

Furthermore, GLNPO.NET users cannot use or access any PII. The PII is only available to system administrators with Domain Admin level access privileges. It is stored in a Windows Active Directory database where there is no primary identifier used for retrieval. Depending on the situation, an administrator may retrieve information using an account username, the user's actual name, or by the user's email address. For example, if a user's password has expired, he or she may provide the account username, and the administrator will locate the account in order to reset the password. Alternatively, if the user has forgotten his or her account username, the administrator may need to search by the user's name or email address to locate and provide the account username.

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?

GLNPO.NET regulate granting of user permissions and depending on permissions granted, the application allows or restricts access to the information to ensure that you have limited the access to the people who have a need to know in the performance of their official duties.

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:

The risk is low/minimal of misuse of information due to the access control levels used by the application. User rights, permissions, and group associations are in place. Access control to user records is governed by user rights, permissions, and security group membership, which is managed by the Account Manager.

Mitigation:

GLNPO.NET has access control procedures in place to regulate granting of user permissions and depending on permissions granted, the application allows or restricts access to the 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: