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: PeoplePlus (PPL)	
Preparer: Mark Leinemann	**Office: OCFO/OTS/IMSD**
Date: 12.13.23	**Phone: 240-559-8624**
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:

PeoplePlus (PPL), a COTS (Oracle) product modified and maintained by EPA Employees and Contractors, is an EPA major information system (MIS). PPL is the EPA's Time and Attendance system. The PPL Absence Management Module has also been implemented for all EPA employees to use PPL for leave management.

PeoplePlus (PPL) supports the EPA's Office of the Chief Financial Officer (OCFO) in the timely and accurate completion of employee Time and Attendance (T&A) to be used for the completion of payroll payments by the EPA's payroll provider and for the submission of employee absence requests.

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?

Pay and Allowances: Purpose - 5 U.S.C. 5101 et seq.; Disposition of Money - 5 U.S.C. 5501 et seq.; Allotment and assignment of pay - 5 U.S.C. 5525 et seq.; Travel, Transportation, and Subsistence Definitions - 5 U.S.C. 5701 et seq.; Attendance and Leave Definitions - 5 U.S.C. 6301 et seq.; Executive agency accounting and other financial management reports and plans - 31 U.S.C. 3512; Use of Social Security Numbers - Executive Order 9397 (Nov. 22, 1943); Government Organization and Employees - 5 U.S.C. 6362; Payment of tax by commercially acceptable means - 5 U.S.C. 6311.

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 04/29/2025

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. An Information Collection Request (ICR) is not required becuause the information is being collected from EPA employees and not from the public.

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).

PPL collects the following: Elements (Hours/Time Reporting Code/Work Code) associated with bi-weekly time and attendance, as well as, elements (Start-End Dates/Leave Category/Absence Type/Duration) associated with the submission of absence requests for various types of leave. Besides the information PPL collects, PPL contains employee: Names, SSNs, EINs, Financial, DOBs, Addresses, Work Telephone #s, Employee IDs

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

The origin of the information comes directly from the employee. The information that PPL collects is entered directly into PPL by the employee. The information that PPL contains that is not entered directly by the employee is downloaded from EPA's payroll provider.

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.

PPL confirms to the greatest extent practicable upon collection of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information utilizing the following process:

PeoplePlus only stores and processes PII and is not responsible for the collection of the PII data. The source system is responsible for confirming the accuracy, relevance, timeliness, and completeness of the PII; collecting the PII directly from the individual to the greatest extent practicable; and checking for, and corrects as necessary, any inaccurate or outdated PII.

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:

Privacy information that is downloaded from EPA's payroll provider may be compromised.

Mitigation:

Server encryption, network firewalls, multi-factor user access, security background checks of individuals who have system access to the PII.

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 does have access control levels within the system that are role-based. EPA employees enter, attest and submit their time in PeoplePlus. Supervisors are responsible for approving employee timecards and have the ability to enter time on behalf of the employees when needed. Timekeepers are responsible for verifying the accuracy of the Time & Attendance data on employee's timecards and have the ability to enter time on behalf of the employee when needed. PeoplePlus Coordinators are responsible for verifying access requested by employees aligns with assigned responsibilities, office needs, and management control principles.undergos a background screening and are assigned a LAN ID and password, they have access to the system.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The users must log into the system and they are assigned a specific role. PeoplePlus (PPL) utilizes a role-based authorization strategy to provide the greatest level for administrative control and scalability. Access to operations within the PPL application is secured based on the role of the authenticated user provided by the System Administrator. The role-based authorization can be fully configured by the System Administrator based on EPA's requirements. Further, the access controls are documented in the PPL's SSP.

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

Yes. PPL Coordinator accounts are created separately: 1) The main EPA PPL Coordinator, who trains and approves others to become PPL coordinators. 2) Office Directors appoint PPL coordinators within their organization. 3) All appointments of PPL coordinators must be approved by the main EPA PPL Coordinator. Accounts are reviewed on a monthly basis.

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 -- PPL Help Desk Analyst, Database Support Analyst and Developers. Contractors do not have access to the live system.

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.

Records are maintained for 5 or more years to allow corrections to be made. The EPA Records Schedule for PeoplePlus is 0300.

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:

There could be a possibility of a data breach during retainment.

Mitigation:

The servers are encrypted, there are network firewalls in place, multi-factor authentication is used for user access, and security background checks of individuals who have system access to the PII are performed.

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.

Yes. Via secure file transfer with IBC over a Multiprotocol Layer Switching (MPLS) interconnection. It is used to process EPA employee payroll.

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

The SORN notes that information is shared with the EPA payroll provider. Without this sharing, EPA employees won't be paid.

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?

It follows procedures set out by NIST 800-53 and EPA's CIO Security Procedures which clarify NIST 800-53.

4.4 Does the agreement place limitations on re-dissemination?

Yes.

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:

The privacy information that is downloaded from EPA's payroll provider may be compromised if shared with an outside source that does not own the data or have a need to know.

Mitigation:

Ensuring individuals signed the National Rules of Behavior prior to access to the system should reduce the likelihood of information being shared to outside sources without a need to know. Users are not allowed by the system to share information that does not belong to them. Any data sent from PPL is encrypted.

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)?

PPL is used internally to maintain and store pertinent employee's time and attendance. PPL users enter information for the sole purpose of Federal Employees' pay. The system ensures that the information is used in accordance with stated practices based on the users acceptance and guidance of the Security Rules of Behavior, and due to the system enforcing role-based functionality. The role-based infrastructure ensures the protection of unauthorized changes. Administrative rights are in place based on the role to trace any changes that are made.

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

In order to maintain their access, all users must attend all required information security and privacy awareness training sessions as well as read and adhere to the Security Rules of Behavior for PPL Users.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Compromised data may not be captured if an inproper/untimely audit is performed.

Mitigation:

Annual third-party sufficient assessments are in place to ensure PPL data controls are in line with NIST 800-53.

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.

PPL uses the information it contains to ensure that EPA employees are paid in a timely and accurate manner and to track employee absences.

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.*)

EPA Network User ID and Employee ID are used to retrieve information.

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EPA-1

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 possibility that the privacy information that is downloaded from EPA's payroll provider may be compromised and used for unauthorized uses.

Mitigation:

Secure file (e.g. encypt, password protect or lock) after it has been downloaded. This should prevent unauthorized access.

*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, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA e, Attn: Privacy Officer, MC 2831T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

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?

Once you become an EPA employee the system is required in order to process an individual's pay. The information provider can decline or opt out of providing this information but in doing so, they can not get their pay processed. Employees get paid, based on their time recorded in the system.

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:

Notices may not provide enough information for users to understand the full uses of their information.

Mitigation:

Ensure that the collection notice provides adequate information for users to understand all of the uses for the collection.

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?

Persons seeking access to their own personal information in this system of records will be required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card) and, if necessary, proof of authority. Additional identity verification procedures may be required as warranted. Requests must meet the requirements of EPA regulations 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. Requests must be submitted to the agency contact indicated on the initial document for which the related contested record was submitted.

8.3 How does the system notify individuals about the procedures for correcting their information?

Any individual who wants to know whether this system of records contain a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA Privacy Officer, MC2831T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

8.4 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:

An individual not properly verified receives personnel information that do not belong to him/her.

Mitigation:

The Agency's Processing Privacy Act Requests Procedure (CIO 2151-P-08.0) applies regarding requests for access and correction to records.