

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: Payment Tracking System (PTS)	System Owner: Adil Gulamali
Preparer: Andrew Lam	Office: OFA/OCIO
Date: 05.08.2026	Phone: 202.564.2925
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 <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 Payment Tracking System (PTS) supports the EPA's Office of Finance and Administration (OFA) in the timely and accurate completion of non-payroll related payments. PTS allows the EPA national finance centers to process Contract, Small Purchase, Interagency, Fellowship, and Grant payments, as well as to track other closely related non-payroll payment information for the EPA. PTS also allows EPA personnel outside of the finance centers to authorize the finance centers to make contract payments. PTS is a modular feeder system to Compass.

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 - 5 U.S.C. 5101 et seq.; Disposition of money accruing from lapsed salaries or unused appropriations for salaries - 5 U.S.C. 5501 et seq.; Allotment and assignment of pay - 5 U.S.C. 5525 et seq.; Definitions: Pay and Allowances - 5 U.S.C. 5701 et seq.; Definitions: Attendance and Leave - 5 U.S.C. 6301 et seq.; Executive agency accounting and other financial management reports and plans - 31 U.S.C. 3512; Executive Order 9397 (Nov. 22, 1943); General authority: Attendance and Leave - 5 U.S.C. 6362; General authority: Attendance and Leave - 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?

PTS has a system security plan and an approved Authorization-to-Operate (ATO). PTS ATO expires on 03.31.2027.

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, the information is not covered by the Paperwork Reduction Act; 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 data will not be maintained or stored in the Cloud.

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).

PTS collects the following information:

Name, Address, Email, Phone number.

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

The information is collected by the EPA Project Officer and is transferred into PTS via Compass which receives the information via Treasury's Automated Standard Application for Payments (ASAP) system and EPA's Next Generation Grant System (NGGS).

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 public available data.

2.4 Discuss how accuracy of the data is ensured.

The EPA Project Officer has the provider of the information verifying said information.

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 provided by the grantee is inaccurate.

Mitigation:

Inaccurate information by the grantee will result in no payment being made. EPA Project Officer must review the provided information thoroughly and validate for discrepancies and requests the provider to make necessary corrections.

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 controls that are role-based. Through the use of multiple roles, each user is limited in what actions they can take and what information they can see while a payment is processed.

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

Each finance center maintains Standard Operating Procedures (SOPs) that define what actions each role can complete. Specifically, for Grant/Fellowship payments; the RTP Finance Center (RTP-FC) maintains the Grant Payment Allocation System (GPAS) Procedures document.

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

Yes, the PTS system incorporates role-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is

identified by the employee's supervisor and approved by regional/national system administrators and then the Payment Tracking System Security Administrator. There are no other users other than the authorized users.

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, PTS Help Desk Analysts (Contractors only), Database Support Analysts (Contractors only) and Developers (EPA employees and Contractors).

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 6 years and 3 months after final payment. They are deleted when no longer needed. PTS has an EPA Records Control Schedule (RCS) and the RCS for PTS is 1005.

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 data stored in PTS are kept active in the system for too long.

Mitigation:

To mitigate the risk of over-retention in PTS, records are kept for up to six years and three months after final payment and then deleted. During the retention period, hard-copy transaction records are stored in a secure, access-controlled room limited to personnel with a need to know. These hard copies are also destroyed according to a defined retention schedule.

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 share outside of EPA is not a part of the normal agency operation.

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

The original purpose of PTS includes the timely and accurate completion of non-payroll related payments. The external sharing with CitiBank, CLPSS and Treasury support payment related activities.

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?

MOUs are reviewed by the Information Security Officer (ISO) with the approval of the Senior Information Official (SIO) and the Chief Information Officer (CIO).

4.4 Does the agreement place limitations on re-dissemination?

Yes. Use of data is covered in the MOU between interconnecting systems.

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:

Information shared outside of the agency may be compromised if handled inappropriately.

Mitigation:

MOU between EPA and outside agencies describe the PII within the information system and the purposes for its distribution and how the data should be protected. To mitigate the risk of information being shared inappropriately; EPA users must take the Security and Privacy Awareness Training to ensure that they understand EPA privacy responsibilities and procedures.

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?

Individuals that have access to this system agree to use the system strictly for the purpose of collection. PTS users that access PTS information resources are required to accept by signature the PTS Rules of Behavior. All users are subject to security controls and roles in the system. They all have at least a basic National Agency Check with Inquiries (NACI) background screening. All EPA personnel with access to sensitive data are required to undergo a higher level of background screening sponsored by EPA. PTS employs role-based access and the principle of least privilege, granting users only the minimum rights needed to perform their tasks—no more and only for as long as necessary.

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

EPA personnel and contractors are required to complete an Information Security and Privacy Awareness and Training course on an annual basis. The training course instructs personnel to not disseminate PII information to unauthorized individuals and how to secure information using approved techniques such as encryption.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Unauthorized user accessing the system or a user who tries to access any data in PTS.

Mitigation:

The PTS system incorporates least privileged access controls that limit the users' rights by what information they need to review or activities they need to perform. PTS user's role is identified by the employee's supervisor and approved by regional/national system administrators and then the PTS system Security Administrator.

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.

PTS (GPAS Module) uses the information to pay fellowship grants. The other modules that comprise PTS do not use PII.

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.) Last name and assigned vendor 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?

[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.]

There is a standard operating procedure (SOP) that has been developed to enforce the sole use and purpose of collection. Individuals that have access to this system agree to use the system strictly for the purpose of collection.

All users are subject to security controls and roles in the system. They all have at least a basic National Agency Check with Inquiries (NACI) background screening. All EPA personnel with access to sensitive data are required to undergo a higher level of background screening sponsored by EPA. PTS employs role-based access and the principle of least privilege, granting users only the minimum rights needed to perform their tasks—no more and only for as long as necessary.

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:

Users mishandle PTS PII.

Mitigation:

To reduce the likelihood of mishandling of PII in PTS, Security and Privacy Awareness Training is provided to ensure that personnel understand privacy responsibilities and procedures. EPA personnel and contractors are required to complete an Information Security and Privacy Awareness training course on an annual basis. The training course instructs personnel to not disseminate PII to unauthorized individuals, how to secure information using approved techniques such as encryption, and proper destruction and disposal of PII. Individuals who have system access must have a security background check. PTS only grants access to users based on the principle of least privilege which provides user sufficient access to perform their jobs, no higher than necessary to accomplish their organizational missions/business functions.

***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.

The system does not provide individuals notice prior to the collection of information. Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

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. Complete EPA Privacy Act procedures are set out in 40 C.F.R. part 16.

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:

There is a notification procedure outline in SORN EPA-29

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, 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. 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:

Individuals' records could be provided to the incorrect requestor.

Mitigation:

EPA's Privacy Act request process ensures the requestor give appropriate identification during a Privacy Act and/or FOIA Request before EPA can share any records that EPA may maintain on that individual.

I attest as the Agency Privacy Officer that **Payment Tracking System (PTS)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA