United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

System Name: Payment Tracking System (PTS)	**System Owner: Michael Clanton**
Preparer: Dennis W. Nachtrieb, Esq.	**Office: OCFO/OTS**
Date: 06.04.2021	**Phone: 919.541.5606**
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 Payment Tracking System (PTS) supports the EPA's Office of the Chief Financial Officer (OCFO) 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?

Yes. 07.30.2021

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).

PTS collects the following: Name, Address, Email, Phone.

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 grantee. The information is collected by the EPA Project Officer and is transfered into PTS via Compass which receives the information via Treasury's Automated Standard Application for Payments (ASAP) system and EPA's Integrated Grant Management System (IGMS).

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.

The EPA Project Officer has the provider of the information verify 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:

Information by the grantee is checked for accuracy by both the EPA finance center payment processor and the EPA finance center payment certifier.

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

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 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 6 years and 3 months after final payment. They are deleted when no longer needed. Yes. RCS 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:

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.

No.

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

N/A

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?

N/A

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:

N/A

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?

The system ensures that the information is used in accordance with stated practices based on the user's acceptance and guidance of the Security Rules of Behavior, and due to the system enforcing role-based functionality.

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 security and privacy awareness training sessions as well as read and adhere to the Security Rules of Behavior for PTS users.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Compromise data may not be captured if an improper audit is performed.

Mitigation:

Annual third-party sufficient assessments are in place to ensure PTS 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.

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. Although, the system indicate that is requires a SORN, the system is covered under the EPA-29 SORN.

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

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 information is used for something other than completing grantee fellowship payments.

Mitigation:

Multiple roles are used to enter/review the information to assure it is handled properly.

***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, 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?

The individual can turn down the fellowship grant / commuting cost reimbursement.

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:

To ensure that the collection notice provide 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?

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:

None. The Agency's Processing Privacy Act Requests Procedure (CIO 2151-P-08.0) applies regarding requests for correction to records.

Mitigation:

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