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: Purchase Card Order Request System (PCORS)	
Preparer: Dina Castellon	**Office: Office of Mission Support (OMS)**
Date: 7/20/20	**Phone: 202-564-4912**
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ 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:

PCORS is an application that is currently implemented on the Agency's Business Automation Platform; The Business Automation Platform, the Agency's implementation of Salesforce Inc.'s **force.com** application Platform as a Service (PaaS), is the Agency's strategic platform for business process automation. PCORS is therefore accessible through https://forms.epa.gov and https://epaoei.lightning.force.com/lightning/page/home.

PCORS was designed for the pre-approval of purchase card transactions and is used to place orders on purchase cards that have already been acquired. Requesters are able to submit their purchase card requests in PCORS (Interface 1). Requests are then routed to the purchase cardholder (PCH) for an initial review, followed by the cardholder's approving official (AO), and finally the Funds Certifying Officer (FCO) for

funding before notifying the cardholder that the request is Fully Approved – Ready to Order status. The PCH, AO, and FCO are the three mandatory approvers on each purchase request though other roles are available as well as options.

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?

- Executive Order 12072 (Aug. 16, 1978);
- Federal Property and Administrative Services Act of 1949, 40 U.S.C. 121;
- Executive Order 9397 (Nov. 22, 1943). 42 U.S.C. 290dd-1, 290ee-1; 5 U.S.C. 7901;
- Executive Order 12564 (Sept. 15, 1986).
- Office of Federal Procurement Policy Act of 1974, 41 U.S.C. 414.
- Public Law 107-67, Section 630
- Executive Order 9397.5 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;
- The Telework Enhancement Act of 2010 (December 9, 2010); and
- Public Law 111–292.

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?

The Agency's Business Automation Platform (BAP) has EPA Authority to Operate at the FISMA Moderate level. It expires September 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?

The EPA's Business Automation Platform (BAP), powered by the Salesforce Force.com Platform as a Service (PaaS), is a shared multi-tenant environment hosted in the Salesforce GovCloud.

The BAP is built specifically on the Salesforce Government Cloud, which is a cloud-hosted, PaaS environment that meets the unique security needs of the Federal Government, including FedRAMP, NIST, and DISA IL2 (IL4 pending

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).

Name

Office/Lab

Branch

Address

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

User input

Enterprise Identity Data Warehouse (EIDW) – Managed by the Agency's Enterprise IT Service Desk (EISD)
Federal Personnel and Payroll System (FPPS) – Managed by the US Department of the Interior

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

Field	Description	Type	Method of Collection	Comments
Requester	name of the requester	auto-populated	EIDW; EPA Locator	Contact's First Name + Middle Name + Preferred Name + Last Name sourced from Enterprise Identity Data Warehouse (EIDW). Preferred Name may be sourced from EPA Locator.

Office/Lab	location of the requester	auto-populated	EIDW; FPPS	Contact's Region or Office, derived from the Contact's HR Org code and Federal Personnel and Payroll System (FPPS) Organization Description. If an Organization is not found in FPPS, the highest level organization is sourced from EIDW.
Branch	organizational information of the requestor	auto-populated	EIDW; FPPS	Contact's Region or Office, derived from the Contact's HR Org code and Federal Personnel and Payroll System (FPPS) Organization Description. If an Organization is not found in FPPS, the highest level organization is sourced from EIDW.
EPEAT Link	a link that directs the user to a webpage that explains what EPEAT is	link	n/a	**link to external site:** https://greenelectronicscouncil.org/epeat/epeat-overview/
Link to IMO Reference List		link	n/a	**link to document on SharePoint site:** https://usepa.sharepoint.com/sites/oei_Community/CIOSAC/Documents/Admin/Member%20List/Official%20CIO%20SAC-SIO-IMO-SITL%20List.pdf
SAM Link	a link to the SAM site	link	n/a	**link to external site**: https://www.sam.gov/SAM/

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data is maintained by the entities the data is sourced from. As data is updated in the source systems, the new data updates the BAP in the regular process of data migration via ETL. Users of the system are responsible for validating the information and actions associated with their requests in PCORS. Users are directed to contact the appropriate help desk when assistance is needed beyond their level of access.

Enterprise Identity Data Warehouse (EIDW) – Managed by the Agency's Enterprise IT Service Desk (EISD)

Federal Personnel and Payroll System (FPPS) – Managed by the US Department of the Interior

EPEAT Site Link – Managed by the Green Electronics Council

IMO Reference List – Managed by the EPA CIO's Senior Advisory Council

System for Award Management (SAM) – Managed by U.S. General Services Administration

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:

There is a low risk of having the information collected disclosed to unauthorized users if the security controls implemented within the BAP were ever breached.

Mitigation:

Currently, only those with valid EPA LAN credentials have access to the BAP. As part of the Enterprise Single Sign-On (ESSO) initiative, EPA users can now use their PIV cards to login to the BAP without needing to enter their User ID and Password. This is accomplished by using Kerberos, a centralized authentication protocol. There are also access control levels that limit users' view/edit access to purchase requests that are either their own or assigned to them for review/approval.

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.

Requester Access: The BAP, and therefore PCORS, currently functions using two interfaces. In the first interface, requesters submit purchase card requests in PCORS and they only have access to view/modify the requests they've submitted. Their identity is verified using their LAN credentials or ESSO. Everyone with valid LAN credentials has access as a requester in PCORS.

Approving Access: The second interface also requires valid LAN credentials or ESSO to access. The second interface limits access to users who perform approving action on a purchase request. This level of access is monitored by the PCORS Application Owner and the BAP Admins. Users requesting this level of access must submit a BAP Provisioning Form requesting the access and providing a justification. Afterwards, the request is reviewed/approved by the PCORS Application owner and then granted by the BAP Admins.

Approvers only have the ability of fully viewing, editing, and approving requests in which they have an active role despite being able to search across all PCORS requests. There is a

master PCORS report that is made available to those with approving access. This master report includes a summarized view of all purchase requests initiated and submitted within PCORS. Users have the ability of duplicating this report and customizing the fields and filters to meet their reporting needs. Despite having the potential of viewing the details of others' purchase requests through this view, they still can't fully view and edit the request unless they are a part of the request's approval chain.

Admin Access: Currently, admin access is granted to the PCORS Development Team, Help Desk, Application Owner, and Purchase Card Team. They have the ability of viewing and modifying fields within all requests in PCORS.

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

Access control is documented within our PCORS User Guide. The user guide is available upon accessing PCORS at the top of the application.

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

Not now though we may create additional permission groups in the future. We have documented the need for other levels of access from 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?

The PCORS Development Team does consist of contractors. The contract did include the appropriate FAR clauses.

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.

The BAP is NOT an approved record-keeping system. BAP contains no records currently. Users agree to this as part of the login process to the BAP. As a platform, it would fall under EPA Records Schedule 1012 – Information and Technology Management.

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 is a risk users may not export the data from PCORS for their records. Records of pre-approval are mandatory to successfully complete the reconciliation of a transaction in

CitiManager.

Mitigation:

No records in the BAP are being deleted at this time unless done so by the user themselves. If there is a need to delete records due to limited storage capacity, the oldest requests will be deleted first, and users will be notified in advance to give them the opportunity to export their purchase request data.

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.

Other organizations, such as the Office of Inspector General (OIG), Government Accountability Office (GAO), or Office of Management and Budget (OMB) may be involved in purchase card oversight. Information is uploaded into CitiManager for transaction reconciliation. CitiManager is the record and reconciliation system for purchase card holders and their approvers. Actual transactions processed on a bank card are recorded in CitiManager and each transaction requires the final approval and acknowledgement of a cardholder's approver before being paid.

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

The Purchase Card Team will work with these organizations to ensure that information is shared, irregularities are identified and investigated, fraud and abuse are eliminated or prosecuted, and that suggested program enhancements in the oversight area are jointly discussed regarding their development and implementation.

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?

There currently aren't any agreements in place nor is there integrated information sharing across organizations. The only way information would be shared would be through a user's actions outside of PCORS since users with elevated access have the ability of customizing and exporting the PCORS master report that is currently made available to them.

4.4 Does the agreement place limitations on re-dissemination?

No

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 is a risk of unauthorized sharing of information since users with approving access have the ability of viewing the information of others through the PCORS Master Report and exporting the data.

Mitigation:

Users will be advised to only export data for record keeping, transaction reconciliation, and workload management purposes only. Future trainings and the PCORS User Guide will be updated to include this rule of behavior.

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?

Through the levels of approval required to complete a purchase card request as well as through periodic audits performed by the Purchase Card Team.

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

EPA Employees must take the Agency's Information Security and Privacy Awareness Training annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of unaccounted for changes/data due to the current limitation the system has to track changes.

Mitigation:

We do ensure changes can only be made by the person it is currently assigned to or a BAP Admin. Those with BAP Admin access have been instructed by the Application owner and BAP COR to never approve on behalf of someone. This has been communicated verbally and via email. They predominately assist in reassigning requests when the person assigned is out of office; the email requesting the change is captured in the approval history when doing so. They encourage users to make changes themselves and try to limit their actions to instructing users.

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.

The system collects the necessary information for the pre-approval of a purchase card transaction in accordance with purchase card policy. It uses the information to validate the requester, all approvers, vendor information, shipping information, and item details. It also uses the information to ensure the request does not exceed the defined purchase card transaction limit.

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.*)

Name and EPA Order Request ID (form ID); users are able to retrieve information from the system based on their name (identified through single-sign on) or by looking up the request ID (which is automatically generated upon its creation by the system).

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 information of individuals is protected using user authentication to access any information in PCORS.

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:

1. There is a risk of requesters not knowing who their purchase card requests should be routed to and the incorrect people will have access to process a request.

2. There is a risk of the purchase card holder, or approvers, not knowing how to use PCORS in accordance with purchase card policy.

Mitigation:

1. Requesters are directed to confirm with their management what their approval chain is. The purchase request is also routed to the cardholder first for an initial review. During this initial review, the cardholder has the ability of reviewing the request, ensuring it's complete, and changing the subsequent approvers if necessary. Approvers have been encouraged to reject requests that are initiated outside of their organization except for unique circumstances.

2. Questions directly related to the implementation of PCORS and how it relates to purchase card policy are deferred to the Purchase Card Team.

***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.

Users are made aware their information is required upon onboarding for proper access to Agency systems and to be included in payroll.

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?

Users are not provided with the opportunity to decline to provide information or opt out of the collection or sharing of their information. PCORS users are aware that, as part of their job, contract data associated with them will be managed and tracked. If EPA personnel do not want to utilize PCORS, they do not have to, however, they may not be able to perform assigned job duties.

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:

PCORS users are not provided with notice prior to their information being collected.

Mitigation:

We can include in training and the PCORS User Guide the statement that "Use of PCORS, implies consent to the collection of the information provided."

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?

The BAP recognizes who is accessing the system through single-sign on. Users are able to retrieve their information by accessing either the "My Orders" option in the Type 1 interface or looking up their name or Order Request ID through the Type 3 interface.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Users are able to contact the PCORS Help desk if they witness inaccurate information. From there, the PCORS Help Desk triages whether it's an issue they can address or directs the user to the correct source.

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:

There is an appropriate process for redress.

Mitigation:

None.