

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: EPA Acquisition System (EAS)	
Preparer: Richard Belles	Office: OMS-ARM/OAS
Date: June 2, 2021	Phone: (202) 564-4339
Reason for Submittal: New PIA ____ Revised PIA __X__ Annual Review ____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/>	
Operation & Maintenance <input type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
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 Office of Acquisition Solutions (OAS) EPA Acquisition System (EAS) is used to initiate, award, modify and track acquisition actions. EAS identifies employees who initiate acquisition actions or are assigned to work on these actions. EAS contains employee name, work email, work telephone and LAN UserID (EAS does not contain any sensitive PII information).

The new EPA Acquisition System (EAS) SaaS will be a cloud-based solution that will replace the old on-premises version. There only change to the system is changing location to a cloud-based Software as a Service (SaaS) solution.

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 EAS SaaS will have a new SSP based on the security plan that has been completed for the EAS. There will be a new ATO for EAS SaaS but there is a valid ATO in place for the existing EAS, expiration date 9/5/2022.

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. The CSP will be FedRamp approved and will provide SaaS.

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 EAS contains employee name, work email, work telephone number, EPA employee ID and LAN UserID. Vendor information including Vendor Code, Legal Name, DUNS ID, Cage Code and address (to identify vendor), Vendor Contact information including Name, phone #, Fax # and email address is also collected.

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

EPA Employee information is collected from the EPA's Active directory. Vendor information is collected from the Federal Government's System for Award Management (SAM).

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

Yes, the Federal Government's SAM is used to collect accurate vendor information. The information collected from SAM is used to identify vendors registered in SAM so they can be selected as sources for a purchase request or contract award etc.

2.4 Discuss how accuracy of the data is ensured.

EAS relies on the EPA's Active Directory and SAM to collect accurate data for EPA users and vendors.

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:

The information is contained on, or is transported over, the EAS contains PII. Due to the information of EPA names, work addresses, work phone, EPA employee ID and LAN UserID and vendor information Vendor Data Universal Numbering System (DUNS) number and Vendor Tax Id Number (TIN), the potential of a breach could exist. If this information was breached or compromised, it could have a low risk of harm to the individual's professional aspects of life.

Mitigation:

Mitigations to protect Privacy include technical, physical, and administration controls. The users of the information are provided Privacy, Security, and Rules of Behavior training on an annual basis. The Agency has a Chief Information Officer (CIO), Information Security Officer (ISO), and Privacy Officer on staff to assist and monitor in protecting the individual's information. Users of the information are only given access to electronic and paper documents that are needed to complete their duty tasks.

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, there are three levels of users: EAS user, EAS Site Admin and EAS Admins. EAS uses role-based access controls to control user access levels.

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

EAS uses role-based access security controls to determine access. There are 3 roles in EAS, 1) EAS user, 2) EAS Site administrators and 3) EAS Administrators. EAS users only have access to the information contained in an action they are assigned to. EAS Site administrators have access to the actions for the site they administer. EAS Administrators have access to all actions.

EAS User roles are documented in the following documents:

- SOP for EAS User Setup – COR.doc
- SOP for EAS User Setup – CO-Warrant Upgrade.doc
- SOP for EAS User Setup – CS.doc
- SOP for EAS User Setup – FCO.doc
- SOP for EAS User Setup – Requisitioner.doc

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

There are no other components with assigned roles and responsibilities within the system.

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?

Authorized authenticated Agency employees and contractors have access to EAS. Appropriate FAR clauses contained in the pertinent contracts govern use by 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.

Information is retained as long as needed to administer the contract. Record schedule # 0055 – Contracts Management Systems

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:

Retention schedule is variable depending on the type of contract or action. Information retained could be subject to breach, loss, or unintentional destruction from external, internal, and physical risks.

Mitigation:

EAS follows Record schedule # 0055 – Contracts Management Systems. The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed. The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy. A process of centralized storage for the facility is being reviewed.

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.

PII is not shared externally. Information is shared with General Services Administration (GSA) Federal Procurement Data System (FPDS) Next Generation (NG). Normal agency requirements to report agency data through the FPDS NG (BetaSam.gov). The FPDS NG is one of the systems maintained by GSA's Integrated Award Environment (IAE) that is used to navigate the federal acquisition lifecycle. One of the most common user activities on FPDS is running reports that provide a range of federal procurement data, called "FPDS reports."

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

PII is not shared externally. The EAS system tracks EPA acquisitions information. Only information required for the purpose of reporting EPA spending is shared.

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?

PII is not shared outside of the EPA. Information sharing agreements will be reviewed and approved in accordance with EPA procedures. ISAs are reviewed by the EAS Information System Security Officer (ISSO) and System Owner before review and approval by the OMS Senior Information Official (SIO).

ISAs are in place between EAS and OCFO's systems 1) Compass and 2) PTS. An interagency agreement between EPA and GSA has been uploaded to Xacta.

- Integrated Award Environment (IAE) | GSA [IAE-EPA-2019-AA]

4.4 Does the agreement place limitations on re-dissemination?

PII is not shared externally. The approved ISA and interagency agreement will place limitation on re-dissemination.

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:

PII could be inadvertently transferred to the interconnecting system via the automated transfer process.

Mitigation:

The current interface has a defined set of data fields that are transmitted, none of which contain PII. The data fields mapping has been documented and uploaded to Xacta. In the event GSA requires changes, the vendor and EPA are notified. The vendor makes the applicable changes and EPA tests the environment prior to release. Relevant security and privacy documentation will be updated, as applicable.

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?

EAS access is limited to authenticated, registered EPA employees with assigned roles and responsibilities. EAS has audit trails for account login, account changes and security (role assignment) changes

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

The Information Security and Privacy Awareness Training is required each year. The course includes information regarding policies and practices that EPA users should follow. The Privacy Act of 1974 and Rules of Behaviors are also discussed.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

If a system does not have technical controls and policy based on safeguarding security measure that can be audited. Not ensuring users are being held accountable for compliance with policy regarding access to a system may present a risk.

Mitigation:

The source systems have access controls and audit trails for grant and procurement information. Users of the systems, as well as users of EAS, must take the Rules of Behavior yearly to maintain access to the system.

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.

EPA user information is used to identify who creates, modifies, owns and has access to actions in EAS.

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.)*

The EAS system is used by acquisition personnel to track the acquisition requirements for the procurement of EPA goods and services. Based on assigned roles, users are able to retrieve information using the Name of EPA employee or Vendor ID (DUNS code). Users ability to view information is limited to their role and assigned users. Information retrieved by name is used to determine the POCs for procurement documentation.

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?

System personnel have reviewed the privacy information contained (Work e-mail, Work phone number, LAN User ID, Name) and method of collection (Active Directory) to determine the effect of privacy on individuals. To mitigate these concerns, PII collected has been limited to only that which is necessary to aid in account management duties. Users with access to privacy information have been limited in accordance to their assigned roles and responsibilities. In addition, all EAS users are EPA employees and contractors and receive Information Security and Privacy Awareness training (ISPAT) within 30 days of hire and annually thereafter. The EAS is configured to audit user activity and leverages EPA enterprise intrusion detection solutions to protect privacy information.

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 risk of an individual not receiving notifications pertaining to acquisition actions when the record contains incorrect information. Incorrect vendor information documented in a record could result in improper dissemination of information.

Mitigation:

Access to EAS is limited to authenticated and registered EPA users who have completed the Rules and Behavior and annual cybersecurity awareness and privacy training. EPA user information is authenticated against the EPA's Active Directory system.

***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?

PII is obtained using information collected from Active Directory. Users are not provided with the opportunity to decline to provide information or opt out of the collection or sharing of their information. EAS users are aware that, as part of their job, contract data associated with them will be managed and tracked. And, users are provided with accounts only at their request. If EPA personnel do not want to utilize EAS, they do not have to submit an account request. However, they will not be able to perform assigned job duties. EPA provides notice prior to obtaining information for use within the agency active directory system, which is used by the EAS system for account management.

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:

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

Mitigation:

OMS/ARM/OAS intends to create an annual privacy notice requirement for new and existing EAS users. Users will digitally sign approval of PII collection requirements, which will be maintained by the office for record.

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 EAS will leverage the established procedures to provide redress.

Mitigation:

N/A