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: CAEDINT, CAEDEXT, and TOCAR	
Preparer: Larry Koss	**Office: Enforcement and Compliance Assurance Division**
Date: 03/23/2020	**Phone: 214-665-6533**
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:

All three systems are housed in RTP on separate servers.

The CAEDINT system houses 10 Oracle APEX Applications that maintain Enforcement and Project information. These applications maintain EPA employees' names and EPA email addresses. That is the only PII data being used.

The CAEDEXT system houses two Oracle Apex Applications that maintains information that is required by EPA from outside sources that are required to report to EPA. These applications maintain EPA employee' names and EPA email addresses. These applications also maintain contact names and emails of individuals submitting the information.

The TOCAR system houses one Oracle Apex Application that maintains Inspection and Enforcement Reports that EPA is required by law to publish to the public. This application does have EPA employee name and email contact information listed.

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?

The CAEDINT and CAEDEXT systems were started inhouse to streamline the Inspection and enforcement processes. The TOCAR system was started under H.R.5150 - Transparency in Government Act of 2019. All three are also covered under E-Government Act [includes FISMA] (P.L. 107-347), Paperwork Reduction Act of 1995 (44 U.S.C. 3501), and H.R.5150 - Transparency in Government Act of 2019. All three systems are also covered under EPA Strategic Plan 2018 – 2022, Greater Certainty, Compliance, and Effectiveness, Objective 3.4 Streamline and Modernize and Objective 3.5 Improve Efficiency and Effectiveness.

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?

All three systems were given an ATO in 2008. Updated ATO in process.

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).

CAEDINT: EPA employee name and EPA email address.

CAEDEXT: EPA employee name and EPA email address. Contact Name and email address.

TOCAR: EPA employee name and EPA email address.

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

CAEDINT: EPA employee name and EPA email address taken from EPA National Locator or Enterprise Identity Data Warehouse (EIDW).

CAEDEXT: EPA employee name and EPA email address taken from EPA National Locator or Enterprise Identity Data Warehouse (EIDW). Contact Name and email entered by the contact person.

TOCAR: EPA employee name and EPA email address taken from EPA National Locator or Enterprise Identity Data Warehouse (EIDW).

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.

Accuracy is maintained by National Locator or EIDW for EPA information. Contact information is checked by the EPA employee receiving the 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:

CAEDINT: Low risk of data entry sending information to the wrong person.

CAEDEXT: Low risk of data entry sending information to the wrong person. Applications are available only to EPA employees with LAN access and registered users. Registered users only have minimal access to their own information.

TOCAR: Low Risk as this is data required to be published. This data contains EPA contact names and EPA emails address for the public to pose questions or request further information. This information can also be retrieved via the EPA pubic web site.

Mitigation:

Use of data maintained in the CAEDINT system is addressed in the EPA Rules of Behavior for EPA users. These Rules of Behavior and repercussions associated with violations of them are addressed during the in-person training and supervisor meetings. Audit logs are controlled and maintained by RTP to assist in violations.

CAEDEXT system uses a warning notice that data submitted is correct prior to submission.

TOCAR system uses Audit logs that are controlled and maintained by RTP to assist in any attempts to unauthorized access.

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?

CAEDINT: Several applications have restrictions where employees can only view data but not edit it. System also uses Audit logs that are controlled and maintained by RTP to assist in any attempts to unauthorized access.

CAEDEXT: Registered users only have access to their data. System also uses Audit logs that are controlled and maintained by RTP to assist in any attempts to unauthorized access.

TOCAR: Is read-only data. System also uses Audit logs that are controlled and maintained by RTP to assist in any attempts to unauthorized access.

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

System documentation maintains any level of access control other than access via LDAP.

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

CAEDINT, CAEDEXT have added assigned roles as need to limit access or changing of data.

TOCAR is read only.

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?

CAEDINT and CAEDEXT: EPA employees or registered users. Only RTP support contractors may have access as part of their administrative duties. RTP contractors are hired by and controlled by RTP EPA personnel and control the FAR clause in their contracts.

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.

EPA Records Schedule 0089. Data is maintained until no longer used and deleted from the system.

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:

Low risk as data may be deleted.

Mitigation:

Retention and Deletion are addressed in the EPA Rules of Behavior for EPA users. These Rules of Behavior and repercussions associated with violations of them are addressed during the in-person training and supervisor meetings. Audit logs are controlled and maintained by RTP to assist in violations.

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.

The information is not shared.

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:

None. Information is not share

Mitigation:

None

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?

Access controls are built in using LAN access.

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

Online training and group training by Supervisor.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low Risk because RTP maintains the Auditing logs.

Mitigation:

Audit logs are controlled and maintained by RTP to assist in accountability.

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 information is collected and used by EPA employees in their work.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X_. 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 information is retrieved by Project Name.

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.]

Data collected is used in the investigation or enforcement of EPA Regulations or Public Laws.

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:

Low Risk for information is misused.

Mitigation:

Use of the information is addressed in the EPA Rules of Behavior for EPA users. These Rules of Behavior and repercussions associated with violations of them are addressed during the in-person training and supervisor meetings.

*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.

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?

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:

Mitigation:

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?

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

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:

Mitigation: