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: Central Data Exchange	
Preparer: Joe Carioti	**Office: OMS/OIM/IESD**
Date: 5/28/2020	**Phone: 202-564-6413**
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:

Central Data Exchange, also known as CDX, is an Environmental Protection Agency (EPA) management information system (MIS). CDX also has Web interfaces used as EPA's Node(s) on the Environmental Information Exchange Network (Exchange Network) to allow companies, states, tribes, local governments and other entities the capability to securely and reliably transfer environmental data in and out of the Agency.

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?

In accordance with the Government Paperwork Elimination Act (44 U.S.C. 3504), EPA's

electronic compliance filing and environmental data exchange system will enable the "acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures." Section 3504(a)(1)(B)(vi) of Title 44, United States Code.

CDX also supports the requirements and procedures set forth under the EPA's Cross-Media Electronic Reporting Rule (CROMERR), which provides the legal framework for electronic reporting under EPA's regulatory programs.

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. The CDX SSP is stored in EPA's XACTA system. CDX received the ATO on October 5, 2016 with expiration extended to October 10, 2020.

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.

OMB Control No. 2025-0025

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. Microsoft Azure Commercial and Government cloud services are used within CDX. Both are FedRAMP approved and used for PaaS and IaaS.

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 CDX environment contains the following data: individual's name, self-assigned user name, security password, work address, work contact information (e.g., phone and fax numbers, E-mail address), and an individual's EPA Program ID and role related to electronically filed reports.

CDX supports a security password reset functionality by collecting and storing a user's 10-

digit cell phone number or a set of secret answers that only the user and the CDX help desk can see. For cell phone numbers, CDX stores other system-generated data such as the authorization code that users must provide when attempting to complete the security password reset process or email validation.

CDX also supports a second-factor authentication feature that uses the same aforementioned 10-digit cell phone number or a set of knowledge-based questions (e.g., what is your favorite TV show) with answers that are hashed in the database for which no one, not even administrators, have access.

CDX offers registrants the option of real time on-line electronic identity verification through a third party service provider (i.e., LexisNexis®). CDX collects, stores, and sends the first name and last name information to LexisNexis for processing and verification; this information is leveraged from the user's account that has already been established. CDX separately collects and sends the following information to LexisNexis for processes and verification, including home address, home phone number, last four of social security number, and date of birth. All of this information is stored as hashes of the information in the database.

CDX stores an individual's self-assigned password created during registration. CDX stores other system-generated data such as the registration date and time, digital certificate identifier, and identifiers used for internal tracking. CDX does not create specific personal identifiers for registrants.

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

CDX maintains records on all individuals attempting to register or registered to obtain an account. Registered CDX users include representatives of industry or government.

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

CDX uses LexisNexis® for identity verification, and this third party service provider uses a proprietary verification process to generate a set of scores ranging from 0 to 12 across various categories (e.g., name-address-social security number or name-address-phone). CDX uses the combination of these scores to define the minimum requirements for passing the verification test per the approval of the CROMERR technical review committee.

2.4 Discuss how accuracy of the data is ensured.

When a new user registers with CDX, the user's email address is verified by sending a confirmation link/code with which the user must respond. Other registration data is verified using LexisNexis Identity Verification services.

CDX supports a paper-based approach for completing identity verification. This can be completed by the EPA program office registration maintenance account manager (RMAM) or CDX's data processing center (DPC); a cost-sharing service available to EPA program

offices.

During the registration process, if the user chooses the paper process for identity verification, the "subscriber agreement" is pre-populated with the information provided by the registrant during account setup (i.e., name, organization name, organization address, User ID). The user is prompted to mail in the signed form, and then placed in a "pending" state without the ability to perform any reporting activities until this information is reviewed and approved by the aforementioned role types.

The processing and verification process will generally consist of verifying the agreement has been filled out and signed, validating the information on the form matches information available from the CDX administrative interface, and a possible phone call to the registrant's company for additional verification before providing the user with access to the program office's reporting application.

Alternatively, for any authorized official who needs to delegate their signing authority to another individual has the option to use CDX's sponsorship module. This module allows for an official from an organization to share this responsibility with an individual online and sign a sponsorship letter to validate this delegation. Upon completion of this delegation process, the user is asked to proceed with the standard registration process that may include the aforementioned paper process.

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:

CDX registration requires submission of personal data such as the user's name and business contact information.

Mitigation:

A warning notice and privacy statement are presented to the user before he or she can login to the CDX website.

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?

CDX has multiple layers of access control built into the system. By default, a non-privileged user only has access to his or her own information. The next layer is called sponsorship, which is the ability for an organizational official to nominate a user (e.g.

subordinate employee or contractor) for access to a program at a level that is lower than their own. Along with granting access, the organization official has the ability to view current and past sponsorships; with the ability to revoke access for users whom access has been granted.

The next access control level is called Registration Maintenance Account Management (RMAM). An RMAM role has access to specific registration, reporting, and security tools for the program that they manage. The registration features that a RMAM has access to include:

- Management of user profiles,
- Creating and pre-registering a user for access to the program,
- Viewing and approving access to their program,
- Viewing their program's role-based access structure,
- Viewing role-based registration activity for their program, and
- Generating a shortcut URL for registration.
- Ability to create alerts and to send emails to users.

The RMAM also has access to view their user's login attempts, password changes, and account statuses.

The last layer of access control is called Helpdesk. Within the Helpdesk layer various roles are used to access to the following features related to user data:

- Ability to generate reports on account and role creation by program for all programs,
- Ability to generate a report on the number of inactivated roles by program for all programs,
- Ability to generate a report on account-specific role status changes by program for all programs,
- Management of user accounts for all programs,
- Ability to approve pending access requests,
- Ability to view login attempts, password changes and account statuses, and
- Ability to create alerts and to send emails to users.

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

CDX access controls are documented within the AC family of security controls of the System Security Plan. For a user to access any data beyond his or her own registration and CDX submissions, permissions must be explicitly granted by the roles described in section 3.1. CDX support personnel, including CDX Help Desk, RMAMs, and System Administrators are required to acknowledge the CDX Rules of Behavior (RoB) before accessing CDX systems. These personnel also receive annual refresher cybersecurity training which includes the proper handling and storage of PII data.

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

No roles other than those described in 3.1 pertain to privacy data.

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?

Government, contractors, and system users will have access to the data/information on CDX. System users will have access to the sponsorship module. The RMAM role access is limited to EPA personnel and contractors supporting the specific program. The Helpdesk roles are limited to contractors and government employees supporting the CDX program. Only personnel with system administrator accounts (who are given more thorough background investigation) can access user data other than their own. The appropriate clauses, as listed above, have been incorporated into the contract and provide a foundation for the contractor's privacy data protection policies.

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.

CDX user data is not purged. However, when accounts are no longer used, they are set to an "expired" state for historical reference and may be reactivated for submissions that occur on an infrequent basis.

The EPA Records Schedule for CDX is 0097 and pertains to program specific information rather than user personal information.

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:

Specific administration and support roles have access to user registration data.

Mitigation:

Rules of Behavior acknowledgement and Security Awareness training are required for key roles.

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.

Yes, CDX is the Agency's portal for exchanging environmental data across heterogeneous systems. Therefore, a primary function of CDX is to connect and to exchange environmental data between EPA program systems and its many external partners, including States, Territories, Tribes, universities, not-for-profit organizations, and others. CDX accomplishes this by participating as a Node in the Exchange Network, where trading partners create agreements stating the kind of data they will share, how frequently they will share it, and in what format it will appear. The Extensible Markup Language (XML) is used to exchange the data to allow compatibility between different systems.

Only environmental data is exchanged using CDX, but a user's name and organizational information may be linked to that data per regulatory requirements.

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

External sharing of environmental data is the primary function of CDX as described within the SORN.

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?

CDX receives written management authorization prior to connecting with other systems and/or sharing data. The CDX environment utilizes Memorandum of Understanding (MOU) and Interconnection System Agreements (ISA) to manage information sharing. CDX has numerous documented interconnections. Each interconnection is documented with a MOU and ISA, which must be reviewed annually.

4.4 Does the agreement place limitations on re-dissemination?

Partners using the Exchange Network and the CDX Node define how they will use data through trading agreements. Those agreements would determine rules for re-dissemination on a case-by-case basis. However, these agreements only apply to environmental data and not to user personal data.

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:

Environmental data submissions that are shared with Exchange Network partner organizations may include the submitter's name and organizational information.

Mitigation:

All information is shared per regulatory requirements and therefore as part of lawful government purposes.

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?

Role-based access controls determine what information can be viewed by a user or administrator. In addition, all user activity is audited within the system and can be viewed according to user by administrators.

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

CDX Administrators and Help Desk representatives are required to take Information Security and Privacy Awareness training and Records Management training on an annual basis.

CDX users are presented with the Warning Notice and Privacy Statement Policy every time they access the main CDX web page.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

No privacy risks related to Auditing and Accountability have been identified.

Mitigation:

N/A

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.

CDX uses data in the following manners:

- **a)** To verify the identity of the individual
- **b)** To investigate possible fraud and verify compliance with Agency program regulations
- **c)** To prepare for litigation or to litigate collection service and audit

CDX collects data to validate CDX users and ensure that they are identifiable by EPA. This EPA practice protects itself, its customers, the CDX environment, and CDX data from the potential impacts of a compromised environment. CDX collects information on EPA's external customers (industry, laboratories, states, etc.). EPA's external customers voluntarily submit compliance data electronically to EPA.

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.*)

Registered users must generate a password to access the system, however CDX staff cannot access the user's self-generated personal password on this system. Registration data is maintained in a secure environment and can only be retrieved by the CDX system management and help desk staff, composed of a very small number of individuals that have undergone specific training and background checks as part of their responsibilities. Data may be retrieved from the system by CDX support personnel through a number of different ways: company address, last name, or other searchable data provided by the registrant at the time of registration.

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?

Privacy data collected is limited to organizational contact information, so personal effect to individuals is minimal, and all data is used per regulatory requirements. Security controls required for an information system rated moderate for confidentiality, integrity, and availability, as prescribed in NIST Special Publication, 800-53, "Recommended Security Controls for Federal Information Systems," Revision 4 are used to protect the privacy data in CDX.

Technical controls include but are not limited to:

- role-based access and authorization,
- system log auditing,
- secure password authentication,
- encrypted transmission of data, and
- network boundary protections and monitoring.

Management controls include but are not limited to:

- user awareness and acknowledgement of rules of behavior regarding system security and privacy and
- system vulnerability scanning and remediation.

Operational controls include but are not limited to:

- security and privacy awareness training,
- establishing and monitoring baseline security configuration of the system,
- configuration control and review with security impact assessment prior to implementation,
- incident response planning,
- physical access control systems,
- personnel background checks, and
- malicious code detection.

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 to information from searches done, only if the information is printed out, and not retrieved immediately.

Mitigation:

All users that have access to information have been trained on protecting user data. For example, if they print something out with sensitive information, it must be picked up from printer immediately.

*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 must access CDX through a "Welcome" web page that includes a warning and links to a Privacy Act Notice that is consistent with federal and EPA standards. See https://cdx.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?

All individuals electing to use CDX are provided advance notice that the use of CDX is voluntary and that they may still opt to use paper or other alternative methods of filing electronically. Also, prior to submitting information, individuals are prompted if they are ready to send or wish to cancel.

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:

No privacy risks related to Notice have been identified.

Mitigation:

N/A

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?

Each CDX user can view his or her full user profile within CDX Web. Users also have their full CROMERR data submission history available to view within CDX Web.

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

Users can edit some user data (e.g., phone number, password, etc.) at any time. The remaining fields can be edited by the CDX Help Desk upon contact by the user. Users can also contact the CDX Help Desk to have their CROMERR data submissions rescinded if necessary.

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:

No privacy risks related to Redress have been identified.

Mitigation:

N/A