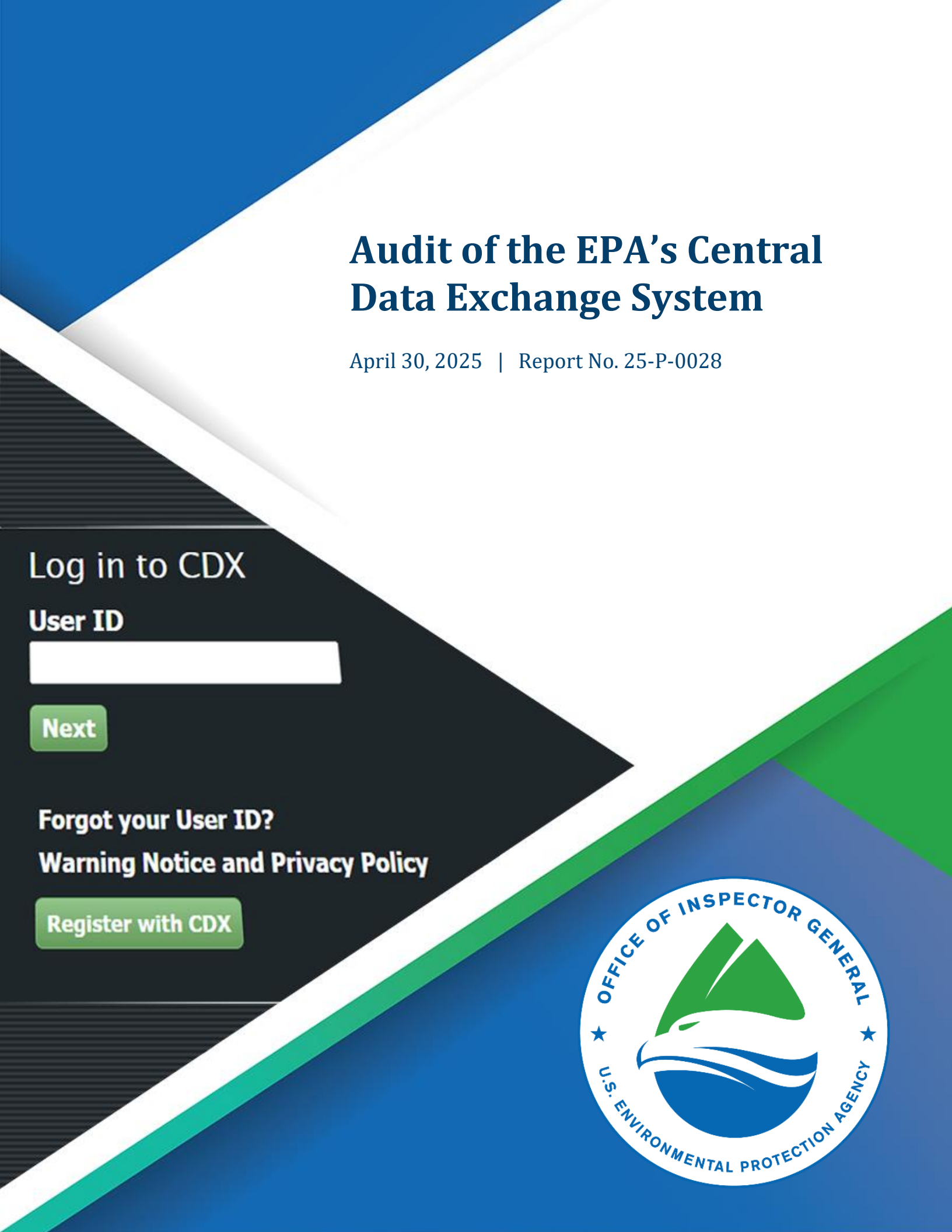
Audit of the EPA's Central Data Exchange System

April 30, 2025 | Report No. 25-P-0028



Report Contributors

Tertia Allen
Yoon An
LaSharn Barnes
Vincent Campbell
Troy Givens
Robert Grayson
Nii-Lantei Lamptey
Iantha Maness
Christina Nelson
Teresa Richardson
Scott Sammons
Michelle Wicker

Abbreviations

CDX	Central Data Exchange
CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
ESA	Electronic Signature Agreement
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OISP	Office of Information Security and Privacy
OPP	Office of Pesticides Program
POA&M	Plan of Action and Milestones
PSP	Pesticide Submission Portal
RMAM	Registration Maintenance Account Manager

Key Definitions

Please see Appendix A for key definitions.

Cover Image

The CDX login screen. (EPA OIG image)

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epaoig.gov

At a Glance

25-P-0028
April 30, 2025

Audit of the EPA's Central Data Exchange System

Why We Did This Audit

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to determine whether the EPA has established sufficient controls to prevent unauthorized access to the Central Data Exchange system.

The Central Data Exchange is a web-based system that allows companies, states, tribes, and other regulated entities to electronically report and transfer their environmental data securely within and outside the EPA. It accepts environmental data for the EPA's air, water, hazardous waste, and toxics release inventory programs, which are sent to one or more of the over 30 program services connected to the system. According to the Office of Mission Support, for fiscal year 2023, the Central Data Exchange system had an operating budget of over $4 million.

To support this EPA mission-related effort:

- *Operating efficiently and effectively.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG.PublicAffairs@epa.gov.

List of OIG reports.

What We Found

The EPA needs to strengthen management and access security controls for the Central Data Exchange, or CDX, system. Specifically, we found that:

- The Office of Pesticide Programs granted 102 non-U.S. users access to the Pesticide Submission Portal without verifying their identities.
- The EPA's account management for the CDX system failed to adhere to the Agency's access control guidance. We identified over 85,000 CDX accounts that were not disabled despite being inactive for over 60 days. We also identified over 100,000 CDX accounts that exceeded the maximum days allowed for user passwords under Agency requirements.
- The CDX system allowed users to input data strings that were not validated for quality and accuracy, such as "aa123<>" listed as a last name and "YOU'REACKED" listed as the username.
- The EPA did not mitigate significant vulnerabilities that an independent security control assessor identified in the *Central Data Exchange Security Assessment Report Continuous Monitoring Assessment – Year 2*, dated March 2022. Although plans of action and milestones were created for these vulnerabilities, the Agency did not review and update the plan of action and milestones in accordance with the Agency's guidance.

The security of the CDX system is integral to the EPA accepting electronic environmental data for the Agency's air, water, hazardous waste, and toxics release inventory programs. Without adequate security controls, the CDX is vulnerable to threat actors exploiting weak security controls to potentially gain unauthorized access, create fraudulent accounts, and enter unreliable data into the system.

Recommendations and Planned Agency Corrective Actions

We initially made 11 recommendations to the principal deputy assistant administrator for Mission Support and two recommendations to the assistant administrator for Chemical Safety and Pollution Prevention regarding the security of the EPA's CDX system. The Agency concurred with seven of our recommendations and provided acceptable corrective actions with estimated milestone dates. In response to Agency comments on the draft report, we revised Recommendation 1 and split responsibility for Recommendation 2. This resulted in an additional recommendation (Recommendation 4) for a total of 12 recommendations for the Office of Mission Support. We consider Recommendations 1, 2, 4, 9, 10, 11, 12, and 14 resolved with corrective actions pending. The six remaining recommendations are unresolved.

April 30, 2025

MEMORANDUM

SUBJECT: Audit of the EPA's Central Data Exchange System Report
No. 25-P-0028

FROM: Nicole N. Murley, Acting Inspector General

TO: Michael Molina, Principal Deputy Assistant Administrator
Office of Mission Support

Nancy Beck, Principal Deputy Assistant Administrator
Office of Chemical Safety and Pollution Prevention

This is our report on the subject audit conducted by the U.S. Environmental Protection Agency Office of Inspector General. The project number for this audit was OA-FY22-0144. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

In accordance with EPA Manual 2750, your office provided acceptable planned corrective actions and estimated milestone dates for Recommendations 1, 2, 4, 9, 10, 11, 12, and 14. We added the current Recommendation 4 in response to the EPA's request, and the former Recommendation 4 became Recommendation 5. The original recommendations you agreed to were numbered 1, 2, 8, 9, 10, 11, and 13 in the draft report. These recommendations are resolved. A final response pertaining to these recommendations is not required; however, if you submit a response, it will be posted on the OIG's website, along with our memorandum commenting on your response.

Action Required

Recommendations 3, 5, 7, 8, and 13—originally numbered 3, 4, 6, 7, and 12—are unresolved. EPA Manual 2750 requires that recommendations be resolved promptly. Therefore, we request that the EPA provide us within 60 days its response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Your response will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epaoig.gov.

Table of Contents

Chapters

-continued-

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency Office of Inspector General initiated this audit to review the EPA's Central Data Exchange, or CDX, access security controls. This audit was the result of several OIG Office of Investigations referrals related to potential systemic issues in the CDX system and its interconnected program applications. Our objective was to determine whether the EPA has established sufficient controls to prevent unauthorized access to the CDX.

Background

The CDX is a web-based system that allows companies, states, tribes, and other regulated entities to electronically report and transfer their environmental data securely within and outside the Agency. The CDX accepts environmental data for the EPA's air, water, hazardous waste, and toxics release inventory programs. The data are sent to one or more of the over 30 program services connected to the CDX, including the Pesticide Submission Portal, or PSP, listed in Appendix B. The environmental data submitted to the CDX must comply with the requirements of the environmental laws that govern the EPA's regulatory responsibilities. For example, companies engaging in pesticides activities must obtain a company number,[1] register, and submit initial and annual pesticides production reports to the EPA in compliance with the Federal Insecticide, Fungicide, and Rodenticide Act. These data are submitted via the PSP within CDX, which the EPA Office of Chemical Safety and Pollution Prevention primarily administers.

CDX Registration

Various stakeholders, such as CDX users, must report environmental data to the EPA. To do so, they must create a CDX account by requesting access to the EPA's environmental program services. Stakeholders are also required to provide identity data, such as an individual or entity name, physical address, email address, and phone number. An EPA employee or contractor serving as the registration maintenance account manager, or RMAM, can assist users with their CDX accounts and program services access, as well as with other administrative activities. Per the PSP registration guidance, to complete the registration, the user can either have a third-party identity verification service electronically verify the user's identity or the user can print, sign, and mail a copy of a paper application—also called an electronic signature agreement, or ESA—to the EPA. Non-U.S. entities are required to designate a U.S.-based authorized agent and print, sign, and mail the ESA to the EPA. An RMAM uses the printed ESA to verify the identity data entered into the CDX and may conduct further

[1] A company number is a unique identifier assigned to a company that wishes to register a pesticide with the EPA.

verification if needed. Once the regulated entity's identity is verified, the RMAM grants it access to the program services or environmental system.

According to the CDX guidance, there are two type of user roles:

RMAM User—Grants access and assigns user privileges or access rights.

CDX User/Regulatory User/Regulatory Entity—Submits environmental information to the EPA.

The OIG Office of Investigations Reported Fraudulent CDX Accounts

In 2021, the OIG Office of Audit received three referrals from the Office of Investigations citing instances of potential identity fraud activity within the CDX and other EPA applications, including the PSP. The Office of Investigations also discovered that the Office of Pesticide Programs, or OPP, granted 102 non-U.S. CDX users access to the PSP without verifying their identities as the EPA's guidance requires. In November 2021, the Office of Investigations alerted the Office of Audit to the potentially fraudulent activity involving the 102 users and the PSP, which occurred after users registered in the CDX system and requested access to the PSP. The Office of Investigations indicated that the potentially fraudulent activity may create an opportunity for identity fraud like the three incidents that the office had previously shared with the Office of Audit. The Office of Investigations also discovered discrepancies in the review and approval process for ESAs. This issue is discussed in Chapter 2.

Federal and Agency Requirements

Below are the federal and Agency requirements that are relevant to our audit.

- The *CDX Pesticide Submissions Portal (PSP) Registration User Guide,* dated August 25, 2020, states that a user's identity must be verified. For non-U.S. users, a CDX RMAM must receive a hard-copy ESA and verify the identity of the entity before granting access.

- Account management of inactive accounts and password expiration requirements, including:

    - National Institute of Standards and Technology, or NIST, Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, which contains the federal guidance for managing inactive accounts and accounts with password expiration requirements. The guidance states that disabling expired, inactive accounts supports the concepts of least privilege and least functionality, which reduce the attack surface of the system.

    - EPA Chief Information Officer, or CIO, Directive 2120-P-07.3, *Information Security – Identification and Authentication (IA) Procedure*, dated January 30, 2023, which implements the federal guidance for user passwords at the EPA and requires that passwords for systems that do not enforce multifactor authentication have a maximum lifetime of 60 days.

- EPA CIO Directive 2150-P-01.3, *Information Security – Access Control (AC) Procedure,* dated June 8, 2023, which requires system owners of all EPA information and information systems to comply with the user access controls, including reviewing active user accounts. Further, the directive requires moderate impact systems to disable accounts within 15 days after being inactive for 45 days.

- Data quality and integrity requirements, including:
  - NIST Special Publication 1500-7r2, Version 3, dated October 2019, *NIST Big Data Interoperability Framework: Volume 7, Standards Roadmap*, which indicates that cleaning data is the "keystone for data quality," and that data must be cleaned to provide accurate analytic outputs. Additionally, the guidance explains that clean data are free from inconsistencies and when errors, such as incorrect data types, have been addressed.
  - EPA CIO Directive 2150-P-17.3, *Information Security – System and Information Integrity (SI) Procedure*, dated November 21, 2023, which includes guidance for checking the validity of all arguments or input data strings submitted by manual or automated processes.[2]
  - NIST Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, under System and Information Integrity, Information Input Validation, which provides details regarding the control, as follows—"the valid syntax and semantics of system inputs, including character set, length, numerical range, and acceptable values, as well as verifying that inputs match specified definitions for format and content."

- Plans of action and milestones, or POA&Ms, which document the corrective action plans to correct weaknesses or deficiencies noted during the assessment of controls and to reduce or eliminate known vulnerabilities in the system. Relevant requirements include:
  - EPA CIO Directive 2150-P-04.2, *Information Security – Security Assessment and Authorization Procedures,* dated May 27, 2016,[3] which states that system owners are responsible for documenting and managing POA&Ms and updating existing POA&Ms monthly in XACTA, the Agency's tool for managing the POA&M process.
  - *XACTA POA&M Guide*, updated and finalized on February 9, 2024, which requires POA&Ms to include certain fields, including at least one milestone activity and a completion date for each milestone activity. All completed POA&Ms should include sufficient evidence supporting that it is complete. The EPA Office of Information Security

[2] An argument or input string in this case refers to values that are input by an individual or machine.
[3] The CIO directive was updated on June 8, 2023, and renamed *Information Security – Assessment, Authorization and Monitoring (CA) Procedure,* CIO Directive 2150-P-04.3. Our audit considered both versions of the directive.

and Privacy, or OISP, should determine monthly which completed POA&Ms can be closed out.

- All Agency directives that we reviewed include a section stating that waivers may be requested by submitting a business justification and establishing compensating controls[4]. A system owner can submit a Risk Determination Waiver to the OISP for approval. Risk Determination Waivers are reviewed on a case-by-case basis. If OISP rejects a Risk Determination Waiver and the system owner disagrees, the system owner can send the waiver to the chief information officer for further review.

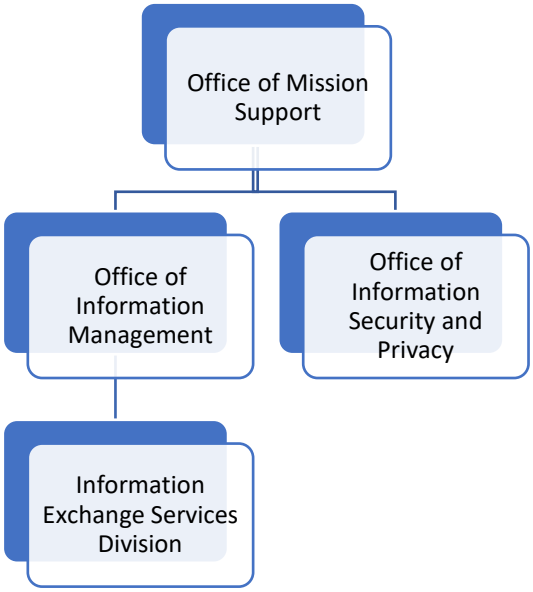
Responsible Offices

The Office of Mission Support, or OMS, manages the CDX program for the Agency and provides EPA programs, states, and tribes, as well as industry, with data exchange options to meet their business needs and comply with the EPA's environmental regulations. The Office of Information Management within the OMS is responsible for operating the CDX, managing the remediation of security vulnerabilities, and managing security controls for CDX passwords and inactive accounts.[5]

Within the OMS, the OISP is responsible for reviewing supporting documentation to validate whether corrective actions remediated the underlying vulnerabilities. The OISP also reviews, approves, or denies risk determination waiver requests that would allow the requester to deviate from Agency policies and procedures. Figure 1 shows the OMS organizational chart.

[4] A compensating control is a control implemented in place of the baseline security control and provides equivalent protection for the system.
[5] The OMS indicated that, as of August 2024, it was no longer responsible for managing CDX passwords and that a third party now has that responsibility. However, the OMS did not provide support for that statement.

Figure 1: Office of Mission Support organizational chart



Source: The EPA. (EPA OIG image)

The OPP within the Office of Chemical Safety and Pollution Prevention regulates the manufacture and use of pesticides—including insecticides, herbicides, rodenticides, disinfectants, and sanitizers—in the United States. The OPP also establishes maximum levels for pesticide residues in food, thereby safeguarding the nation's food supply. Pesticide producers report pesticide activities to the OPP using the CDX system.

According to the OMS, the CDX's fiscal year 2023 budget totaled $4,338,998.75. This amount is meant to fund annual third-party cybersecurity assessments, CDX Web, implementation of the Cross-Media Electronic Reporting Rule, and risk management framework support. The budget also funds other security items such as vulnerability assessments, incident management, and audits.

Scope and Methodology

We conducted this performance audit from August 2022 to December 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the internal controls necessary to satisfy our audit objective.[6] In particular, we assessed the internal control components—as outlined in the U.S. Government Accountability Office's *Standards for*

[6] An entity designs, implements, and operates internal controls to achieve its objectives related to operations, reporting, and compliance. The U.S. Government Accountability Office sets internal control standards for federal entities in GAO-14-704G, *Standards for Internal Control in the Federal Government*, issued September 10, 2014.

Internal Control in the Federal Government—significant to our audit objectives. Any internal control deficiencies we found are discussed in this report. Because our audit was limited to the internal control components deemed significant to our audit objective, it may not have disclosed all internal control deficiencies that may have existed at the time of the audit.

To address our audit objective, we reviewed the CDX's security controls and the integrity of identity data within the CDX's user records. Further, we analyzed the user accounts from one program office the Office of Investigations mentioned in its referrals regarding fraudulent CDX activities. We requested the ESAs that contained the wet-ink signatures for some users who requested access to the PSP program service. We narrowed our scope to the PSP program service because of the Office of Investigations' referrals stating that non-U.S. CDX users were granted access to the PSP. We also surveyed Agency program staff personnel responsible for managing CDX user accounts registered to various program services or data flows.

To further address the audit objective, we obtained an understanding of relevant internal controls intended to remediate security vulnerabilities, as well as CDX password and inactive user account management. We interviewed CDX system staff and OMS policy staff.

We interviewed the CDX system owner and reviewed the CDX security assessment reports from FY 2020, FY 2021, and FY 2022 to gain an understanding of the CDX's security controls.[7] We gained an understanding of the EPA's POA&M process by reviewing Agency guidance and interviewing the CDX system owner and OISP personnel. By obtaining and reviewing screenshots from XACTA, we verified that CDX personnel created POA&Ms for the weaknesses identified in the security assessment reports. We also verified the status of outstanding CDX POA&Ms as of April 2024 created from the security assessment report. We gained an understanding of the risk determination waiver process by interviewing OISP personnel and reviewing the OISP's process for approving risk determination waivers. We also reviewed Agency and federal guidance regarding data integrity and data quality, the evaluation of security controls, and the management of user accounts. In addition, we tested the controls. The OIG Data Analytics Directorate further identified and analyzed data quality and integrity issues, and it assisted with analytical approaches for the CDX user accounts.

The CDX system owner provided spreadsheets that listed all CDX users and RMAMs as of March 2024. We analyzed the spreadsheets to calculate the number of active CDX user and RMAM accounts that should be disabled or locked because of inactivity or password expiration.

Prior Reports

EPA OIG Report No. 24-N-0025, *Central Data Exchange System Identity Data Are Unreliable*, issued on March 5, 2024, identified our concerns regarding questionable data quality and integrity of the CDX identity data entered by CDX registrants and the RMAMs. The report noted our concerns with the

[7] The reports provide a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.

quality and integrity of the identity data in CDX data files that are transferred to the EPA's 30-plus environmental systems that support EPA programs. We made no recommendations in the report.

EPA OIG Report No. 24-N-0024, *Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks*, issued on March 5, 2024, identified our concerns regarding the lack of attention to mitigating significant vulnerabilities within required time frames specified in Agency procedures. The report notes that failure to remediate the vulnerabilities could leave the system open to brute force attacks.[8] Moreover, if they are left uncorrected, the EPA's network would be more vulnerable to threat actors gaining access to the CDX and environmental data that states, tribes, and other entities rely on, as well as to the potential disclosure and modification of data for over 30 program services that are connected to the CDX. We made no recommendations in the report.

[8] A brute force attack is a cyberattack that allows a threat actor to gain unauthorized access to an account by attempting multiple combinations of passwords.

Chapter 2
The EPA Needs to Validate Unverified User Accounts on the CDX System

According to the OIG Office of Investigations, from September 2020 to May 2022, the Office of Pesticide Programs granted 102 non-U.S. users access to the PSP without performing the identity verification that the EPA's guidance requires. According to the OPP's *CDX-Pesticide Submissions Portal (PSP) Registration User Guide*, users who report electronically to the EPA must have their identities verified. The guidance instructs non-U.S. CDX users to complete, print, and mail to the EPA an ESA containing a written signature on company letterhead to serve as identity verification, if required. However, the OPP changed its procedure and is no longer accepting printed ESAs with a written signature for non-U.S. PSP users, leaving OPP with no means of verifying the identity of its non-U.S. users.[9] Contrary to the former procedure, this change in procedure is not documented, and therefore the OPP is not complying with existing guidance that requires verification of identities. This lack of identity verification resulted in potentially fraudulent activity for the PSP program service and the CDX registration system.

The OPP Did Not Comply with Its Guidance for Non-U.S. CDX Users

The OPP granted 102 non-U.S. CDX users access to the PSP without verifying their identities as the EPA's guidance requires. The *OPP CDX Pesticide Submissions Portal (PSP) Registration User Guide,* dated August 25, 2020, states that to request access to the PSP via CDX, a domestic or U.S.-based CDX user must establish and verify its identity either by electronic verification through a third-party or by printing and signing an ESA. Additionally, the guidance requires non-U.S. users to designate a U.S.-based authorized agent, print the ESA, apply a wet-ink signature, and mail the ESA to the EPA. The guidance states that non-U.S. users must wait for the PSP RMAM to receive the ESA and grant access to the user. Because of undocumented changes to the identity verification process and a lack of training for RMAMs, this guidance was not followed. Furthermore, the OIG Office of Investigations alerted the OIG Office of Audit about potentially fraudulent activity involving the PSP, which occurred after users registered in the CDX system and requested access to PSP. The Office of Investigations indicated that the potentially fraudulent activity may create an opportunity for identity fraud.

New Process Was Not Documented

The OPP did not provide documentation of its latest process for verifying the identity of the 102 non-U.S. CDX users requesting access to PSP or those users' ESAs, contradicting its guidance on using printed ESAs for identity verification. The OPP indicated that events, such as mandatory telework during the coronavirus pandemic, prevented it from performing identity verification because OPP staff were unable to receive mailed-in ESAs to review. As a result, OPP management stated that since the

[9] These 102 non-U.S. registrants were part of the OIG Office of Investigations investigation into fraudulent activity regarding the PSP and the Section Seven Tracking System. That system manages information associated with pesticide-producing and device-producing pesticide establishments.

pandemic, the OPP changed its identity verification process and accepted emailed ESAs for identity verification. The OPP also stated that it validates non-U.S. CDX users who request access to the PSP by ensuring that they provide identity information for themselves and their authorized agents. But, since it did not provide ESAs for the 102 non-U.S. CDX users in question, the validity of the users could not be verified. These approved accounts are potentially fraudulent, but the OPP continues to request that users' submissions go through CDX, contrary to the identity verification process documented in EPA guidance.

Lack of Training

In addition to new processes that are undocumented, another factor contributing to the noncompliance is the lack of agencywide CDX registration training for the RMAMs, which could also result in the acceptance of fraudulent accounts. Based on survey results from 59 Agency RMAMs from several program offices, we found that the RMAMs did not have formal training for their RMAM activities. Furthermore, the survey showed that several were unaware of the written procedures that they should be following to register users.

Conclusions

The OPP did not follow its documented procedures, resulting in 102 non-U.S. CDX users whose identities remain unverified. These unverified users gained access to the PSP, which exposes the PSP application and the CDX to the potential for fraudulent information and activities. By not following the documented PSP registration guidance for identity verification, the OPP may be receiving unreliable pesticide information from unverified users, which, if trusted, could be detrimental to human health and the environment.

Recommendations

We recommend that the assistant administrator for Chemical Safety and Pollution Prevention:

1. Verify all unverified account holders and provide a list to the Office of Mission Support to disable unverified accounts.

2. Update the Office of Pesticide Programs' guidance to align with the current identity verification process.

We recommend that the assistant administrator for Mission Support:

3. Develop and implement a documented process for active registration maintenance account managers to acknowledge their roles and responsibilities, including signing the Central Data Exchange Rules of Behavior.

4. Disable accounts that the Office of Chemical Safety and Pollution Prevention identified as unverified.

Agency Response and OIG Assessment

We originally had three recommendations related to this finding. The Agency proposed changes to the original Recommendation 1 to split responsibilities between OMS and the Office of Chemical Safety and Pollution Prevention, also called OCSPP. We agreed, which resulted in adding an additional recommendation to this finding: Recommendation 4.

The Agency agreed with the original Recommendations 1 and 2 and the new Recommendation 4, originally part of Recommendation 1, and provided proposed acceptable planned corrective actions with an estimated completion date of July 1, 2025. Specifically, the Agency said that OCSPP will evaluate all unverified account holders and provide a list of accounts that cannot be verified to the OMS to be disabled as well as update the OPP's guidance for processing user permissions to align with the current identity verification process. In addition, OMS will disable accounts that cannot be verified.

The Agency disagreed with Recommendation 3 and proposed changes to the recommendation that would provide the Agency with flexibility to address this issue in the way that it believes is most effective. We agreed with the Agency's proposed changes and updated our recommendation. We consider this recommendation unresolved.

The Agency's response to our draft report is in Appendix C.

Chapter 3
The EPA Needs to Comply with Its Access Control Requirements

The EPA's account management for the CDX system failed to adhere to Agency information technology access control requirements. We found that the EPA did not manage or monitor privileged and general user accounts, resulting in 34 CDX RMAMs and over half of the 165,867 CDX accounts remaining active after 60 days of inactivity. Additionally, over 100,000 of the CDX accounts, or 62 percent, exceeded the 60-day maximum password lifetime policy requirement. The EPA CIO directives require moderate impact systems to disable accounts within 15 days after being inactive for 45 days and require systems without multifactor authentication to have passwords with a maximum lifetime of 60 days.[10] The CDX system owner stated that the CIO directives excluded regulatory users, which include CDX users, and, as a result, accounts were not regularly reviewed or monitored and were not disabled for inactivity and password expiration. Furthermore, the FY 2024 CDX security assessment report states that the CDX password expiration security controls were inherited from the cloud provider. These inherited controls did not comply with the CIO directives. By not disabling accounts for inactivity and expired passwords, the Agency is exposed to threat actors using these accounts to obtain unauthorized access to the CDX system and potentially to over 30 program services connected to the CDX system.

The EPA Did Not Disable Inactive Accounts in CDX

The EPA did not disable inactive CDX accounts as required by the Agency's access control requirements. We identified that 85,071 CDX users and 34 CDX RMAMs have access to the CDX system and the connected program services, despite not logging into their accounts for over 60 days. According to the *CDX Rules of Behavior*, Version 2.5, dated July 2023, RMAMs are privileged users that grant CDX users access to program services; therefore, it is important that the RMAMs' accounts be disabled promptly, so that threat actors cannot compromise them.

Key Definitions

User: An individual authorized to access a system.

Privileged user: An individual who is authorized and trusted to perform security-relevant functions that ordinary users are not authorized to perform.

Privileged account: A system account with the authorization of a privileged user.

Moderate impact system: A system in which at least one security objective—such as confidentiality, integrity, or availability—is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

EPA CIO Directive 2150-P-01.3, *Information Security – Access Control (AC) Procedure,* requires owners of EPA-operated systems to implement the security controls documented within the procedure. According

[10] As of October 3, 2024, the Agency stated that the CDX system uses multifactor authentication, but we found that the CDX system did not have multifactor authentication.

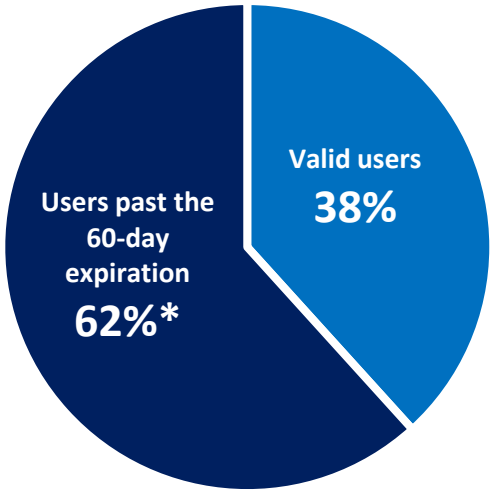
to this directive, moderate impact system accounts should be disabled within 15 days of being inactive for 45 days. Additionally, it states that procedures "address all United States EPA information and information systems to include information and information systems used, managed, or operated by a contractor, another agency, or other organization on behalf of the EPA." According to the OISP, the CIO directives apply to all users, including regulatory entities.

The CDX system owner, however, stated that "[the] scope statement in [CIO Directive 2150-P-01.3] excludes regulatory [CDX] users as they are not providing the information or using the information system on behalf of the EPA—they are performing regulatory requirements." As a result, the accounts were not disabled. Without the EPA disabling all inactive accounts, including those of regulatory entities, users will continue to have access to the CDX system even if they do not need it. Furthermore, disabling inactive accounts reduces the attack surface of the system, which is the number of exposed entry points for a threat actor to use. The smaller the attack surface, the less chance of a threat actor finding a vulnerability and exploiting the system.

The EPA Did Not Lock CDX Accounts that Exceeded Password Expiration Lifetime

The EPA did not consistently enforce the maximum days allowed for a user's password, or password maximum lifetime requirements, in accordance with the Agency's identification and authentication requirements. Our analysis identified that nearly two-thirds of the 165,867 CDX user accounts in early March 2024 remained unlocked after the prescribed 60-day password reset time frame had expired, as seen in Figure 2.

Figure 2: User accounts that remained unlocked after the 60-day password reset time frame and the valid users as of March 11, 2024



* 102,365 user accounts.

Source: OIG analysis of EPA CDX system data. (EPA OIG image)

Furthermore, as shown in Table 1, our analysis showed that 15,132 CDX users, or 9 percent of all users, logged into their accounts after the 60-day expiration date lapsed—in fact, dozens were able to log in nearly a year later.

Table 1: Days of access after the 60-day expiration

Days of access after the 60-day expiration	Number of users
1–60	14,732
61–120	156
121–180	101
181–240	81
241–300	37
301–360	25
Total	**15,132**

Source: OIG analysis of Agency-provided data pulled from the EPA CDX system. (EPA OIG table)

The EPA did not consistently enforce the password expiration. According to the FY 2024 CDX security assessment report, the CDX system owner accepted the password expiration security controls from the cloud provider without verifying that the control met the CIO requirements. The control establishes a maximum password lifetime of 90 days. This is not consistent with EPA CIO Directive 2120-P-07.3, *Information Security – Identification and Authentication (IA) Procedure*, which requires that passwords for systems that do not enforce multifactor authentication shall have a maximum lifetime of 60 days. The procedure is applicable to "all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency" and applies to all EPA employees, contractors, "and all other uses of EPA information and information systems that support the operations and assets of the EPA." In addition to using the cloud provider's password expiration security controls, the CDX system lacks any consistent automated or manual review of CDX password expiration controls to lock accounts that exceed the password lifetime. Poor enforcement of password expiration increases the risks of weakened password security, exposure to credential theft, compliance and audit failures, and potential delays in incident response.

Conclusions

By not disabling inactive accounts or accounts with expired passwords, the EPA's network is vulnerable to threat actors exploiting these weak security controls to potentially gain access to the CDX system and to over 30 program services that are connected to the system. According to the Cybersecurity and Infrastructure Security Agency, threat actors routinely exploit weak security controls to gain unauthorized access to a system. Additionally, the lack of automated or manual reviews of password expiration increases the attack surface in which threat actors can gain access to CDX and all connected program services.

Recommendations

We recommend that the assistant administrator for Mission Support:

5. Disable all Central Data Exchange accounts that are inactive for over 45 days, as required by EPA Chief Information Officer Directive 2150-P-01.3.

6. Develop and implement a documented process to regularly review the activity of Central Data Exchange accounts and disable inactive accounts promptly, as required by EPA Chief Information Officer Directive 2150-P-01.3.

7. Develop and implement a documented process to review and disable Central Data Exchange accounts that exceed the password expiration lifetime set by EPA Chief Information Officer Directive 2120-P-07.3.

8. Train staff responsible for Central Data Exchange account management to implement the inactivity requirements set in the information security awareness training specifically pertaining to EPA Chief Information Officer Directive 2150-P-01.3.

Agency Response and OIG Assessment

The OMS disagreed with these recommendations and did not provide acceptable planned corrective actions or estimated milestone dates. We consider these recommendations unresolved.

For Recommendations 5, 6, and 8, the OMS stated that an IT Security Waiver is in place and that the recommendations should be resolved or removed.[11] As observed during our audit, the OMS submitted several risk determination waiver requests; however, the OISP rejected the waiver requests and indicated that the Agency should resubmit the requests with detailed business justification. In the Agency's response to our draft report, the Agency did not provide evidence that approved waivers were in place; therefore, we consider the Recommendations 5, 6, and 8 unresolved.

For Recommendation 7, the OMS stated that "[p]assword expiration and management has been transitioned to the federal service provider login.gov."[12] The Agency did not provide evidence of this implementation.

The Agency's response to our draft report is in Appendix C.

[11] Our original recommendation numbers changed because we added a new recommendation, as discussed in Chapter 2. Recommendations 5, 6, and 8 were originally Recommendations 4, 5, and 7. The Agency's response, shown in Appendix C, reflects the original recommendation numbers.
[12] Originally, Recommendation 7 was Recommendation 6. The Agency's response references this recommendation as Recommendation 6.

Chapter 4
The EPA Needs to Implement Validation Controls in the CDX System that Prevent Input of Questionable Identity Data

CDX users submitted identity data in the system that did not comply with EPA and federal requirements. Specifically, we saw two identity data files in the CDX system—the CDX user file and the RMAM user file—where no controls were implemented to check the validity of all arguments or input data strings users submitted by manual or automated processes that adhere to Agency guidance. This occurred because the CDX system does not contain system controls to prevent users from entering identity data that are questionable and thus unreliable. Without the EPA having the proper system controls in place, threat actors could create fraudulent CDX accounts that could provide unauthorized access to other EPA systems and environmental data that are used to support the EPA's mission and strategic goals.

The EPA Did Not Follow Data Quality and Integrity Requirements

The CDX system does not contain system controls, as prescribed by federal or Agency requirements, that prevent users from entering questionable identity data. We analyzed the identity data contained in the RMAM and CDX user files. The RMAM file included 1,873 records and contained information such as email addresses and phone numbers. The CDX user file included 195,950 records and contained CDX user identity data such as names, addresses, and organization names. The RMAM and CDX user files contained data that did not meet the quality and integrity requirements outlined in EPA Directive No. 2150-P-17.3 and in the *NIST Big Data Interoperability Framework* guidance. For example, in a CDX user file, we found users with first and last names such as "<i>YOU'REACKED<i>" and "abcdefghijklmn." As another example, in an RMAM file, we identified phone numbers listed as "1231231233." These examples suggest that the CDX system lacked system controls that would validate user-submitted identity data for accuracy or quality. Table 2 illustrates the types of issues we saw in the files.

Table 2: Examples of the issues we identified in the RMAM and CDX user files

Examples	File and field	Issues	Number of issues identified	Percent of records with issues (%)
abc@123.com gmail.com yahoo.com	RMAM file* Email address field	Questionable email addresses. Some emails appear to be personal email addresses used by EPA personnel or those conducting business on the EPA's behalf; however, EPA guidance strongly discourages the use of personal emails.	122	6.51

Examples	File and field	Issues	Number of issues identified	Percent of records with issues (%)
5555555555 1231231233 9999999999	RMAM file* Phone number field	Questionable phone numbers. The data appears to be false because the phone numbers have the same sequence of numbers.	280	14.94
YOU'REACKED aaaaaa aatest<>	CDX user file† First name field	Questionable first names. One name reads "YOU'REACKED." First names rarely have repetitive letters and symbols.	94	0.05
YOU'REACKED abcdefghijklmn aa123<>	CDX user file† Last name field	Questionable last names. Last names rarely have sequenced letters of the alphabet, numbers, or symbols.	79	0.04
CDX Testing Company Test_23 <>marquee 1.00E+11	CDX user file† Organization name field	Questionable organization names with symbols and other noncharacters.	71	0.04
Numbers like 1,2,7,10 Firstname.lastname@163.com xcvxv	CDX user file† Physical address field	Questionable addresses, with entries including personal email addresses instead of physical addresses. Some entries contained numbers with no street names or contained random characters.	599	0.31

* The RMAM file that we reviewed contained 1,873 records.

† The CDX user file that we reviewed contained 195,950 records.

Source: OIG analysis of EPA CDX data. (EPA OIG table)

Because we found that CDX users entered questionable, unrestricted data, we also reviewed the CDX user log data to determine whether CDX users performed other unrestricted activities in the system. During our review, we learned that the CDX system only captures user ID, last login date, registration date, password reset date, password expiration date, account status, program service, and role. The system does not track how often a CDX user account is accessed, what areas within the system the user visits, or what tasks users perform. As a result, the EPA does not have the ability to effectively track user accounts in CDX to determine what activities the questionable users performed.

The EPA did not include safeguards in the CDX system to prevent the input of questionable arguments, also known as data strings, that CDX users entered. EPA CIO Directive 2150-P-17.3, *Information Security – System and Information Integrity (SI) Procedure*, assigns responsibility to the senior information officer, information security officer, system owner, or designees to check the validity of all arguments or input data strings submitted through manual or automated processes. For example, if the organization specifies that numerical values between 1 and 100 are the only acceptable inputs for a field in a given application, inputs of "387," "abc," or "%K%" are invalid inputs and are not acceptable as input to the system. Further, the NIST *Big Data Interoperability* Framework guidance indicates that cleaning data is the "keystone for data quality," and that data must be cleaned to provide accurate analytic outputs.

Specifically, the NIST *Big Data Interoperability* Framework indicates that clean data are free from inconsistencies and errors, such as incorrect data types.

We met with OMS representatives regarding our finding, and they confirmed that there are no controls in CDX to catch questionable data because the system has open text fields. In other words, a CDX user has control over the content and format of the identity data that the user enters in the system. The OMS stated that it does not enter or process the identity data. The OMS indicated in its response to our March 2024 Report No. 24-N-0025, *Central Data Exchange System Identity Data Are Unreliable*, that the program office user registration staff is responsible for ensuring that only authorized users have access to its systems.

The presence of questionable data in the RMAM and CDX user files, along with the identity issues identified in the Office of Investigations' referrals, indicates that the system is vulnerable to both fraudulent activity and other potential threats. Using fraudulent accounts, threat actors could potentially gain access to the CDX and other EPA environmental systems connected to it and enter questionable or fraudulent data that could undermine the credibility of the information these systems aggregate and maintain to support the EPA's program services and strategic plan. Implementing input validation controls would not only protect against such threats but could also prevent malicious acts like cross-site scripting or injection attacks,[13] further protecting the Agency from threat actors.

Conclusions

The EPA relies on the environmental data users to enter information into CDX to help meet the EPA mission to protect human health and the environment. The NIST *Big Data Interoperability* Framework guidance states that not having clean data can lead to inaccurate analytics, incorrect conclusions, and wrong decisions. While we only reviewed the files that contained identity data, it is possible that other CDX files have similar data quality issues. For example, a March 2023 report published by the EPA's Data Governance Council documented challenges with CDX data. The EPA's chief data officer, chief architect, and geospatial information officer facilitated a forum that collected information from the regions and program offices on data-related challenges that the EPA faces with data governance. Our finding related to questionable data and the data-related challenges that the Data Governance Council noted in its report may indicate a correlation as to how our finding reveals the data challenges on getting data to other systems. CDX data are transferred across the EPA's environmental systems and subsequently used by the EPA to make decisions and to make progress toward the EPA's strategic plan goals. If the EPA does not mitigate its CDX data integrity issues, it cannot provide assurance that its environmental data are accurate and reliable.

[13] Cross-site scripting is a vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and the client. An injection attack or SQL injection attack is an attack that looks for websites that pass insufficiently processed user input to database backends.

Recommendations

We recommend that the assistant administrator for Mission Support:

9. Implement a process to assess the validity of the questionable Central Data Exchange identity data currently in the system and disable accounts that contain identity data that cannot be verified.

10. Develop and implement a strategy to comply with federal and Agency system input control requirements for the user identity files in the Central Data Exchange system.

Agency Response and OIG Assessment

The OMS agreed with our recommendations, provided acceptable planned corrective actions, and provided acceptable estimated milestone dates for Recommendations 9 and 10.[14] We consider these recommendations resolved with corrective actions pending.

For Recommendation 9, the OMS stated that it would implement a process to assess the validity of the questionable CDX identity data currently in the system and disable accounts where identity data cannot be verified with a proposed corrective action completion date of May 1, 2025.

For Recommendation 10, the OMS stated that it will develop and implement a strategy to comply with federal and Agency system input control requirements for the user identity files in the CDX system with a proposed corrective action completion date of June 1, 2025.

The Agency's response on our draft report is in Appendix C.

[14] In our draft report, these were Recommendations 8 and 9. The Agency's response in Appendix C references those numbers.

Chapter 5
The EPA Did Not Mitigate Vulnerabilities in the CDX System

The EPA did not mitigate significant vulnerabilities identified in the CDX system. Although the Agency developed POA&Ms for the vulnerabilities, the EPA did not review and update the POA&Ms monthly as required and the EPA did not implement adequate compensating controls to address the risks associated with the unresolved vulnerabilities in the CDX system. Additionally, the EPA did not properly validate the completion of POA&Ms to address the CDX vulnerabilities. Specifically, the Agency closed a POA&M that did not have appropriate security documentation in the XACTA system and did not review security documentation submitted for POA&M closure in a timely manner, as required by the *XACTA POA&M Guide*. These issues occurred because the Agency did not follow its own procedures regarding the POA&M process, the system owner did not update POA&Ms in XACTA due to higher priority work, and the OISP did not include completed POA&Ms with backdated completion dates in its monthly POA&M reports. As a result of the EPA not mitigating significant vulnerabilities for these unresolved POA&Ms, the CDX system is more susceptible to cyberattacks, such as brute force attacks.[15]

The EPA Did Not Resolve CDX Vulnerabilities in a Timely Manner

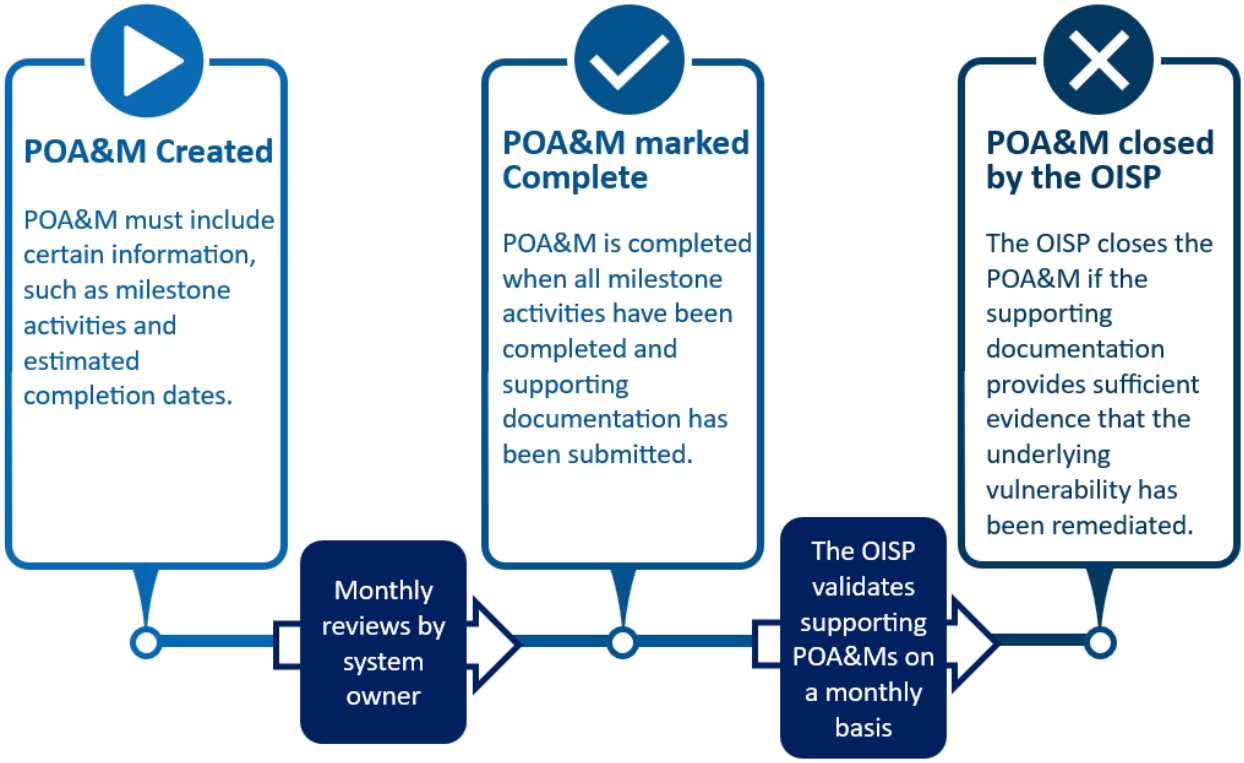
As part of a CDX FY 2022 continuous monitoring assessment, an independent security control assessor team conducted a security assessment of the system. *The Central Data Exchange Security Assessment Report Continuous Monitoring Assessment – Year 2*, dated March 2022, identified 25 vulnerabilities associated with 21 security controls. The Agency developed 20 POA&Ms to remediate the 25 vulnerabilities. In the course of this audit, we issued a management alert to the Agency, Report No. 24-N-0024, *Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks*, that discussed two high-risk and 12 moderate-risk vulnerabilities that remained unresolved as of April 2024. The EPA developed 12 POA&Ms to address these 14 vulnerabilities; however, the POA&Ms did not adhere to the Agency's procedures and guidance. During the course of our audit, the Agency took action to address seven of the 12 CDX POA&Ms.

According to EPA CIO Directive 2150-P-04.2, *Information Security – Security Assessment and Authorization Procedures*, system owners are responsible for developing POA&Ms and updating existing POA&Ms monthly so that there is an accurate record of all planned, in-process, and completed actions to correct deficiencies. Further, the *XACTA POA&M Guide*, updated and finalized on February 9, 2024—during the course of our audit—requires that all POA&Ms include milestones with a completion date, the system owner update XACTA as soon as POA&Ms are completed, and completed POA&Ms include

[15] A brute force attack is a cyberattack that allows a threat actor to gain unauthorized access to an account by attempting multiple combinations of passwords.

sufficient evidence to support that the POA&Ms are completed. The Agency's POA&M process is illustrated in Figure 3.

Figure 3: The POA&M process



Source: *XACTA POA&M Guide*. (EPA OIG graphic)

A POA&M may be considered complete if the Agency accepts the risk, meaning that it is aware of the vulnerability and accepts the risk that it carries. To accept the risk, a system owner must submit a risk determination waiver to the OISP to request an exception from certain EPA information technology procedures. The risk determination wavier should include (1) a detailed business justification explaining why information technology procedures do not need to be followed for a particular situation and (2) information regarding implemented compensating or mitigating controls.

Key Definitions

Compensating control: A control implemented in place of the baseline security control that provides equivalent protection for the system.

Preventive control: An activity designed to prevent a risk from occurring.

Detective control: An activity designed to discover when a risk is occurring.

The CDX submitted five risk determination waiver requests related to vulnerabilities identified in the FY 2022 CDX security assessment report. However, the OISP rejected all five risk determination waiver requests, stating:

> Based on the review of your requests and EPA existing policies and procedures approval is not recommended. If a deviation from the existing policy and procedures is required to support your business needs, please resubmit these requests documenting your detailed business justification and all implemented compensating/mitigating controls deployed to reduce risks from deviating from existing EPA policies and procedures.

In response to the draft report that we issued to the Agency on September 12, 2023, the Agency provided a written description, dated February 13, 2024, of the compensating controls it put in place for the 14 unresolved vulnerabilities from the FY 2022 CDX security assessment report. We did not consider these controls to be compensating controls since they did not protect the system as required by the baseline security controls. For example, we identified that the controls the Agency described were detective and not preventive, and, therefore, would not protect the confidentiality and integrity of transmitted information and prevent unauthorized disclosure or modification of data in the system.

The EPA was not able to track the status of actions taken for these unresolved vulnerabilities because the Agency did not adhere to the POA&M procedures. Although the Agency uses the XACTA system to track POA&Ms, it used another system, Jira, to monitor and track CDX POA&Ms. Our review of the Jira screenshots showed that the POA&Ms were not updated monthly and that corrective actions to resolve the vulnerabilities were not completed. According to the CDX system owner, the XACTA system was not updated monthly due to higher priority work to implement identity credential and access management and multifactor authentication.

By allowing moderate- and high-risk vulnerabilities to remain in the CDX system for over two years, the EPA's network is vulnerable to the risk of threat actors exploiting these vulnerabilities; gaining access to the CDX system and the environmental data that states, tribes, and other entities rely on; or disclosing and modifying data for the other systems that are interconnected to the CDX system.

The EPA Did Not Properly Validate Completion of CDX POA&Ms

The EPA had deficiencies in validating the completion of several CDX POA&Ms. As documented in Report No. 24-N-0024, *Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks*, the OISP closed a POA&M for a password configuration vulnerability without confirming that the security documentation attached in XACTA supported the remediation of the underlying vulnerability. Additionally, we identified that the OISP did not review and validate security documentation attached in XACTA within the required time frame for two POA&Ms that CDX personnel submitted for closure. According to the *XACTA POA&M Guide*, on a monthly basis, the OISP should determine which completed POA&Ms can be closed out.

By prematurely closing a POA&M, the EPA leaves the CDX system vulnerable to brute force attacks. As a result of our audit, the OISP updated the *XACTA POA&M Guide* to Version 5.01, dated February 2024, to include that the OISP must review and validate corrective actions to ensure that a POA&M is not prematurely closed.

Due to a flaw identified in the review process, the OISP overlooked two completed POA&Ms with backdated completion dates and did not perform the closeout actions monthly as required by the *XACTA POA&M Guide*. POA&Ms may use a prior date, like the date of the supporting documentation, as the completion date. The OISP's process for generating monthly POA&M reports does not include POA&Ms with backdated completion dates. In response to our audit, the OISP is reviewing its process for generating monthly POA&M reports to ensure that all POA&Ms marked as completed are reviewed by the OISP in a timely manner.

Conclusions

According to the Cybersecurity and Infrastructure Security Agency, the time between a threat actor discovering a vulnerability and exploiting the vulnerability is decreasing. It reported that, on average, threat actors exploit a vulnerability within 15 days of discovery. Moderate- and high-risk vulnerabilities have continued to remain on the CDX system for over two years after the independent assessor issued its March 2022 security assessment report. Left uncorrected, these vulnerabilities put the EPA's network at greater risk to threat actors exploiting these weaknesses to gain access to the CDX and the environmental data that states, tribes, and other entities rely on, as well as to potential disclosure and modification of data for over 30 program services that are connected to the CDX.

Recommendations

We recommend that the assistant administrator for Mission Support:

11. Develop and implement a process for the system owner to document monthly updates to the XACTA system that includes the current status of completing the milestone activities for the Central Data Exchange system's plans of action and milestones, as required by EPA Chief Information Officer Directive 2150-P-04.3 and the *XACTA POA&M Guide*.

12. Develop a process that includes reviewing all ongoing Central Data Exchange system plans of action and milestones in XACTA to ensure that all fields required by the *XACTA POA&M Guide* are completed, including the milestone activity and scheduled completion date.

13. Remediate the unresolved vulnerabilities identified during the fiscal year 2022 security assessment report for the Central Data Exchange system or obtain risk determination waivers to accept the risk.

14. Develop a documented process to ensure that all completed plans of action and milestones are included in the monthly review described in the *XACTA POA&M Guide* related to validating supporting documentation and closure.

Agency Response and OIG Assessment

The OMS agreed with our recommendations, provided acceptable planned corrective actions, and provided acceptable estimated milestone dates for Recommendations 11, 12, and 14.[16] We consider these recommendations resolved with corrective actions pending.

For Recommendation 11, the OMS stated that it will develop and implement a process for the system owner to document monthly updates to the XACTA system, including the current status of completing milestone activities for the CDX system's POA&Ms. For this corrective action, the Agency provided an estimated completion date of July 1, 2025.

For Recommendation 12, the OMS stated that it will develop a process that includes reviewing all ongoing CDX system POA&Ms in XACTA to ensure that all fields are completed, including the milestone activity and scheduled completion date. The Agency listed August 1, 2025, as the estimated completion date for this corrective action.

For Recommendation 13,[17] the OMS stated that the remediation of open vulnerabilities and POA&Ms is an ongoing process and recommended bounding the recommendation to the 14 POA&Ms identified during the audit. The OIG revised the recommendation to be specific to the vulnerabilities identified during the FY 2022 CDX security assessment report. We consider the recommendation unresolved.

For Recommendation 14,[18] the OMS stated that it would develop a documented process to ensure all completed plans of action and milestones are included in the monthly review and developed a draft standard operating procedure for monitoring and validating POA&Ms. The Agency listed April 15, 2025, as the estimated completion date for these corrective actions. However, we are unable to verify whether the actions have been completed. We will continue to work with the Agency.

The Agency's response to our draft report is in Appendix C.

[16] Originally, these were Recommendations 10, 11, and 13. The Agency's response in Appendix C uses the original numbers.
[17] Originally, this was Recommendation 12. The Agency's response in Appendix C uses the original recommendation number.
[18] Originally, this was Recommendation 13. The Agency's response in Appendix C uses the original recommendation number.

Status of Recommendations

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
1	9	Verify all unverified account holders and provide a list to the Office of Mission Support to disable unverified accounts.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	7/1/25
2	9	Update the Office of Pesticide Programs' guidance to align with the current identity verification process.	R	Assistant Administrator for Chemical Safety and Pollution Prevention	7/1/25
3	9	Develop and implement a documented process for active registration maintenance account managers to acknowledge their roles and responsibilities, including signing the Central Data Exchange Rules of Behavior.	U	Assistant Administrator for Mission Support	—
4	9	Disable accounts that the Office of Chemical Safety and Pollution Prevention identified as unverified.	R	Assistant Administrator for Mission Support	7/1/25
5	14	Disable all Central Data Exchange accounts that are inactive for over 45 days, as required by EPA Chief Information Officer Directive 2150-P-01.3.	U	Assistant Administrator for Mission Support	—
6	14	Develop and implement a documented process to regularly review the activity of Central Data Exchange accounts and disable inactive accounts promptly, as required by EPA Chief Information Officer Directive 2150-P-01.3.	U	Assistant Administrator for Mission Support	—
7	14	Develop and implement a documented process to review and disable Central Data Exchange accounts that exceed the password expiration lifetime set by EPA Chief Information Officer Directive 2120-P-07.3.	U	Assistant Administrator for Mission Support	—
8	14	Train staff responsible for the Central Data Exchange account management to implement the inactivity requirements set in the information security awareness training specifically pertaining to EPA Chief Information Officer Directive 2150-P-01.3.	U	Assistant Administrator for Mission Support	—
9	18	Implement a process to assess the validity of the questionable Central Data Exchange identity data currently in the system and disable accounts that contain identity that data cannot be verified.	R	Assistant Administrator for Mission Support	5/1/25
10	18	Develop and implement a strategy to comply with federal and Agency system input control requirements for the user identity files in the Central Data Exchange system.	R	Assistant Administrator for Mission Support	6/1/25
11	22	Develop and implement a process for the system owner to document monthly updates to the XACTA system that includes the current status of completing the milestone activities for the Central Data Exchange system's plans of action and milestones, as required by EPA Chief Information Officer Directive 2150-P-04.3 and the *XACTA POA&M Guide*.	R	Assistant Administrator for Mission Support	7/1/25
12	22	Develop a process that includes reviewing all ongoing Central Data Exchange system plans of action and milestones in XACTA to ensure that all fields required by the *XACTA POA&M Guide* are completed, including the milestone activity and scheduled completion date.	R	Assistant Administrator for Mission Support	8/1/25

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
13	22	Remediate the unresolved vulnerabilities identified during the fiscal year 2022 security assessment report for the Central Data Exchange system or obtain risk determination waivers to accept the risk.	U	Assistant Administrator for Mission Support	—
14	22	Develop a documented process to ensure that all completed plans of actions and milestones are included in the monthly review described in the *XACTA POA&M Guide* related to validating supporting documentation and closure.	R	Assistant Administrator for Mission Support	4/15/25

* C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

Key Definitions

Brute Force Attack: An attack that allows a threat actor to gain unauthorized access to an account by attempting multiple combinations of passwords.

Compensating Control: A control implemented in place of the baseline security control that provides equivalent protection for the system.

Cross-Site Scripting: A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and the client.

Detective Control: An activity designed to discover when a risk is occurring.

Injection Attack: An injection attack is an attack that looks for websites that pass insufficiently processed user input to database backends.

Moderate Impact System: A system in which at least one security objective—such as confidentiality, integrity, or availability—is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

Plan of Action and Milestones: A document that details the planned corrective action to correct weaknesses or deficiencies noted during the assessment of controls and to reduce or eliminate known vulnerabilities in the system.

Preventive Control: An activity designed to prevent a risk from occurring.

Privileged Account: A system account with the authorization of a privileged user.

Privileged User: An individual that is authorized and trusted to perform security-relevant functions that ordinary users are not authorized to perform.

User: An individual authorized to access a system.

Appendix B

Program Services Connected to the CDX System

1. Aircraft Reporting and Compliance System.
2. Burial at Sea.
3. Combined Air Emissions Reporting.
4. Consent Decree Reporting System.
5. Compliance and Emissions Data Reporting Interface.
6. Submissions for Chemical Safety and Pesticide Programs.
7. Voluntary Disclosure System, known as EDisclosure.
8. General E-Enterprise Use, known as EEP.
9. National Environmental Policy Act NEPA Electronic Filing System, known as e-NEPA.
10. Electronic Permit System.
11. Engines and Vehicles – Compliance Information Systems.
12. Federal Insecticide, Fungicide, and Rodenticide Act Grant Database.
13. Fuel Oil Non-Availability.
14. Federal Air Rules for Reservations Online Reporting System.
15. Great Lakes Environmental Database Query System.
16. Exchange Network Grant Semi-Annual Reporting Forms, known as IEPB.
17. Lead-Based Paint Program, known as LEAD.
18. National Pollutant Discharge Elimination System eReporting Tool.
19. Network Discharge Monitoring Report, known as NetDMR.
20. Ozone Depleting Substances.
21. Office of Transportation Air Quality DC FUEL Program.
22. Office of Transportation and Air Quality EPA Moderated Transaction System.
23. Office of Transportation and Air Quality Fuels Registration.
24. Cellulosic Biofuel Waiver Credits Spay.gov Application, known as OTAQWaiverCredits.
25. Petitions to Object to Title V Permits.
26. Pesticide Submission Portal.
27. Resource Conservation and Recovery Act Information.
28. Risk Management Plan, known as RMPESUBMIT.
29. SPeCS for Exceptional Events, known as S4EE.
30. State Planning Electronic Collaboration System.
31. Substance Registry Service.
32. Section Seven Tracking System.
33. Smartway Technology Application Reporting System.
34. Subpart W Impoundment Photographic Reporting.
35. Toxics Release Inventory Made Easy Web.
36. 2013 Vessel General Permit.
37. Water Contaminant Information Tool.

Agency Response to Draft Report

OFFICE OF MISSION SUPPORT
WASHINGTON, D.C. 20460

January 23, 2025

MEMORANDUM

SUBJECT: Response to the Office of Inspector General Draft Report, Project No. OA-FY23-0061, "*The EPA Needs to Strengthen its Management and Access Security Controls for the Central Data Exchange System*" dated December 19, 2024.

FROM: Vaughn Noga, Chief Information Officer
Deputy Assistant Administrator for Information Technology and Information Management

VAUGHN NOGA
Digitally signed by VAUGHN NOGA
Date: 2025.01.23 19:30:24 -05'00'

TO: Vincent Campbell, Director
Information Resources Management
Office of Audit

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. Following is a summary of the U.S. Environmental Protection Agency's overall position, along with its position on each of the report's recommendations. We have provided high-level corrective actions and estimated completion dates.

AGENCY'S OVERALL POSITION

The draft report contains eleven recommendations for the Office of Mission Support and two for the Assistant Administrator for Chemical Safety and Pollution Prevention. The agency agrees with seven of the recommendations (#'s 1, 2, 8, 9, 10, 11, and 13) and disagrees with six of the recommendations (#'s 3, 4, 5, 6, 7, and 12.

For recommendations the agency disagrees with (#'s 3, 4, 5, 7, and 12), we have provided alternative recommendation language below as well as our reasoning for those proposed

changes. For recommendation #6, this recommendation has already been addressed and should either be removed or marked as resolved in the final report. We have attached a technical comments document to provide additional context and to ensure the accuracy of the report.

AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

Agreements

No.	Recommendation	High-Level Corrective Action(s)	Est. Completion Date
1	Verify all unverified account holders and disable accounts that cannot be verified.	CA 1A: OCSPP will evaluate all unverified account holders and provide a list of accounts that cannot be verified to OMS to be disabled.	July 1, 2025
		CA 1B: OMS will disable accounts that cannot be verified.	July 1, 2025
2	Update Office of Pesticide Programs' guidance to align with the current identity verification process.	CA 2: OCSPP will update the Office of Pesticide Program's guidance for processing user permissions to align with the current identity verification process.	July 1, 2025
8	Implement a process to assess the validity of the questionable Central Data Exchange identity data currently in the system and disable accounts where identity data cannot be verified.	OMS will implement a process to assess the validity of the questionable Central Data Exchange identity data currently in the system and disable accounts where identity data cannot be verified.	May 1, 2025
9	Develop and implement a strategy to comply with federal and Agency system input control requirements for the user identity files in the Central Data Exchange system.	OMS will develop and implement a strategy to comply with federal and Agency system input control requirements for the user identity files in the Central Data Exchange system.	June 1, 2025

10	Develop and implement a process for the system owner to document monthly updates to the XACTA system that includes the current status of completing the milestone activities for the Central Data Exchange system's plans of action and milestones as required by CIO Directive 2150-P-04.3 and the XACTA POA&M Guide.	OMS will develop and implement a process for the system owner to document monthly updates to the XACTA system that includes the current status of completing the milestone activities for the Central Data Exchange system's plans of action and milestones as required by CIO Directive 2150-P-04.3 and the XACTA POA&M Guide.	July 1, 2025
11	Develop a process that includes reviewing all ongoing Central Data Exchange system plans of action and milestones in XACTA to ensure that all fields required by the XACTA POA&M Guide are completed, including the milestone activity and scheduled completion date.	OMS will develop a process that includes reviewing all ongoing Central Data Exchange system plans of action and milestones in XACTA to ensure that all fields required by the XACTA POA&M Guide are completed, including the milestone activity and scheduled completion date.	August 1, 2025
13	Develop a documented process to ensure that all completed plans of action and milestones are included in the monthly review documented in the XACTA POA&M Guide related to validating supporting documentation and closure.	OMS will develop a documented process to ensure that all completed plans of action and milestones are included in the monthly review documented in the XACTA POA&M Guide related to validating supporting documentation and closure. A draft Standard Operating Procedure (SOP) has been developed for monitoring and validating POA&Ms. This draft is currently in review.	April 15, 2025

Disagreements

No.	Recommendation	Agency Explanation/Response	Proposed Alternative
3	Develop and conduct formal training for the EPA's registration maintenance account managers and sign Central Data Exchange Rules of Behavior once the training is complete.	Training is a tool that could be used, but we want to make sure that we have the flexibility to address this issue in the way that is most effective.	OMS will develop a process to ensure that CDX RMAMs understand and acknowledge their roles and responsibilities.
4	Disable all Central Data Exchange accounts that are inactive for over 45 days as required by CIO Directive 2150-P-01.3.		An IT Security Waiver is in place. This recommendation should either be removed or marked as resolved.
5	Develop and implement a documented process to regularly review the activity of Central Data Exchange accounts and disable inactive accounts promptly as required by CIO Directive 2150-P-01.3.		An IT Security Waiver is in place. This recommendation should either be removed or marked as resolved.
6	Develop and implement a documented process to review and disable Central Data Exchange accounts that exceed the password expiration lifetime set by CIO Directive 2120-P-07.3.	This recommendation is no longer applicable.	OMS - Password expiration and management has been transitioned to the federal service provider login.gov. This recommendation should either be removed or marked as resolved.

7	Train staff responsible for the Central Data Exchange account management to implement the inactivity requirements set in the information security awareness training specifically pertaining to CIO Directive 2150-P-01.3.		An IT Security Waiver for account inactivity is in place. This recommendation should either be removed or marked as resolved.
12	Resolve the vulnerabilities on the Central Data Exchange system or obtain Risk Determination Waivers to accept the risk.	During the audit, CDX continued to remediate open vulnerabilities and POA&Ms. Of the original 14 identified vulnerabilities, OMS has resolved all but 2 which are large in scope. OMS recommends bounding this action to the POA&Ms identified during the audit because vulnerabilities and POA&Ms are part of an ongoing process to identify remediations to risks.	OMS will remediate the 14 unremediated vulnerabilities identified at the onset of this audit on the Central Data Exchange system or obtain Risk Determination Waivers to accept the risk.

CONTACT INFORMATION

Thank you again for the opportunity to review the report. If you have any questions regarding this response, please contact Afreeka Wilson, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564-0867 or wilson.afreeka@epa.gov.

ATTACHMENTS

1. CDX Draft Report Technical Comments

cc: Vincent Campbell
Tertia Allen
Yoon An
Troy Givens
Robert Grayson
Nii-Lantei Lamptey Iantha
Maness Christina Nelson
Teresa Richardson Scott
Sammons Michelle

Wicker
Erin Collard
David Alvarado
Austin Henderson
Jennie Campbell
Dwane Young
Joe Carioti
Tonya Manning
Mark Bacharach
Lee Kelly
Kaitlyn Khan
Janet Weiner
Rachel Holloman
Daniel Rosenblatt
Hayley Hughes
Karen Fligger
Robert Schultz
Edward Messina
Leo Gueriguian
Elizabeth Vizard
Rashawd Smith
Kimberly Smith
Daniel Schoeff
Yulia Kalikhman
Gregory Scott
Jan Jablonski
Justin Bossard
Afreeka Wilson
Darryl Perez
Susan Perkins
Andrew LeBlanc
Jose Kercado-Deleon

Appendix D

Distribution

The Administrator
Deputy Administrator
Assistant Deputy Administrator
Associate Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Principal Deputy Associate Administrator for Public Affairs
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Audit Follow-Up Coordinator, Office of the Administrator
Office of Policy GAO Liaison
Office of Policy OIG Liaison
Assistant Administrator for Mission Support
Assistant Administrator for Chemical Safety and Pollution Prevention
Principal Deputy Assistant Administrator for Mission Support
Principal Deputy Assistant Administrator for Chemical and Safety Prevention
Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management, Office of Mission Support
Director, Office of Information Security and Privacy, Office of Mission Support
Deputy Assistant Administrator for Workforce Solution and Inclusive Excellence, Office of Mission Support
Deputy Assistant Administrator for Infrastructure and Extramural Resources, Office of Mission Support
Director, Office of Resources and Business Operations, Office of Mission Support
Audit Follow-Up Coordinator, Office of Mission Support
Senior Advisor, Office of Chemical Safety and Pollution Prevention
Deputy Administrator, Office of Chemical Safety and Pollution Prevention
Deputy Administrator for Management, Office of Chemical Safety and Pollution Prevention
Senior Audit Advisor, Office of Chemical Safety and Pollution Prevention
Director, Office of Pesticide Programs, Office of Chemical Safety and Pollution Prevention

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit the OIG's whistleblower protection webpage.

Contact us:

Congressional & Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X: @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov