Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks

March 5, 2024 | Report No. 24-N-0024

me to the Environmental Protection Agency (EPA) Central Data Exchange (C
l Data Exchange concept has been defined as a central point which su
xisting functions for receiving legally acceptable data in various fo

proceeding and accessing U.S. Government
of the following:

you are accessing U.S. Go
unauthorized access
administrative
the term
you

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Report Contributors

Tertia Allen
Yoon An
LaSharn Barnes
Troy Givens
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
OIG	Office of Inspector General
POA&M	Plan of Action and Milestones

Key Definitions

Brute Force Attack — Allows a threat actor to gain unauthorized access to an account by attempting multiple combinations of passwords.

Plan of Action and Milestones — Documents the corrective action plans to correct weaknesses or deficiencies noted during the assessment of controls and to reduce or eliminate known vulnerabilities in a system.

Cover Image

The Central Data Exchange is the EPA’s electronic reporting site for environmental data. (EPA OIG adaptation of EPA images)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740

OIG.Hotline@epa.gov

Learn more about our OIG Hotline.

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

Subscribe to our Email Updates.
Follow us on X (formerly Twitter) @EPAoig.
Send us your Project Suggestions.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

March 5, 2024

MEMORANDUM

SUBJECT: Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks
Report No. 24-N-0024

FROM: Sean W. O'Donnell, Inspector General Sean W O'Donnell

TO: Kimberly Patrick, Principal Deputy Assistant Administrator
Office of Mission Support

The U.S. Environmental Protection Agency Office of Inspector General initiated an audit to review the EPA's Central Data Exchange, or CDX, system's access security controls. While conducting work on that audit, which remains ongoing, we decided to issue this management alert to inform the Agency of significant unresolved vulnerabilities in the CDX system. These vulnerabilities increase the risk of threat actors gaining unauthorized access to CDX and other connected program services. Additionally, we are alerting the Agency of deficiencies in validating the completion of the CDX plans of action and milestones, or POA&Ms, for several vulnerabilities.

This management alert supports an EPA mission-related effort:

- Operating efficiently and effectively.

This management alert addresses a top EPA management challenge:

- Managing grants, contracts, and data systems.

You are not required to respond to this management alert because it contains no recommendations. If you submit a response, however, it 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 accessibility 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 management alert to our website at www.epaoig.gov.

Background

The CDX is a web-based system that allows companies, states, tribes, and other entities to electronically report and transfer their environmental data securely within and outside the Agency. The CDX collects environmental data for the EPA's air, water, hazardous waste, and toxics release inventory programs. The system allows end users to create accounts in the CDX and provides identity verification services to enable access to over 30 program services, such as systems and tools. According to the CDX registration webpage, a user can register for available program services to access through the CDX. Additionally, the EPA uses the information maintained in the CDX to investigate potential fraud involving a registered user; verify compliance with program regulations; and initiate legal action regarding program fraud, abuse, or noncompliance.

The security of EPA information and information systems is vital to the success of the EPA's mission. Therefore, the EPA conducts periodic testing and evaluates security controls for every system to ensure that security controls are working as intended. As part of the CDX fiscal year 2022 continuous monitoring assessment, an independent Security Control Assessor Test Team conducted a security assessment of the CDX system. A security assessment determines the extent to which security controls are correctly implemented, are operating as intended, and are producing the desired outcome to meet the system requirements. The resulting report, *The Central Data Exchange Security Assessment Report Continuous Monitoring Assessment – Year 2*, dated March 2022, included test results for not just the fiscal year 2022 assessment but also the fiscal years 2020 and 2021 assessments. It identified 25 vulnerabilities associated with 21 security controls. Two of the 25 identified vulnerabilities were categorized as high risk, while 23 were categorized as moderate risk. Vulnerabilities categorized as high risk may have a catastrophic impact on an organization's operations or systems, and vulnerabilities categorized as moderate risk may have serious adverse impacts on an organization's operations or systems.

The Agency developed 20 POA&Ms for the 25 vulnerabilities; 12 POA&Ms associated with 14 vulnerabilities remained open as of August 2023.[1] The National Institute of Standards and Technology Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Revision 2, dated December 2018, states that system owners prepare POA&Ms based on the findings and recommendations of the security assessment reports. The purpose of these POA&Ms is to 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.

Responsible Offices

The EPA Office of Mission Support owns the CDX. The Office of Information Management, a program office within the Office of Mission Support, is responsible for operating the CDX. The CDX system owner

[1] The Agency closed six POA&Ms, and two POA&Ms were submitted for closure as of August 2023.

is responsible for reviewing and updating the POA&Ms monthly. The system owner or other CDX system personnel upload supporting documentation to the Agency's Information Security Repository system, known as XACTA, to support the closure of these POA&Ms. The Office of Information Security and Privacy, a program office within the Office of Mission Support, is responsible for reviewing the POA&Ms' supporting documentation to validate whether the corrective actions remediated the underlying vulnerability and for closing the POA&Ms within the XACTA system.

Scope and Methodology

We conducted our work from August 2022 to September 2023. While our overall audit, which is still ongoing, is being conducted in accordance with generally accepted government auditing standards, the work related to this management alert does not constitute an audit done in accordance with these standards. However, we did follow the OIG's quality control procedures for ensuring that the information in this report is accurate and supported.

OIG Concerns

The EPA did not mitigate significant vulnerabilities identified in the CDX system. During the fiscal year 2022 security assessment of the CDX system, the Security Control Assessor Test Team identified vulnerabilities in the system, which the Agency did not remediate within the required time frames, as identified in the Agency's *Information Security – Security Assessment and Authorization Procedures*, CIO 2150-P-04.2, dated May 27, 2016. The Agency should remediate vulnerabilities within either a 30-, 60-, or 90-day time frame based on the severity of the vulnerability.

Of the 25 identified vulnerabilities, two high-risk and 12 moderate-risk vulnerabilities remained unresolved as of August 2023. Although the Agency developed POA&Ms for these vulnerabilities, it did not adhere to CIO 2150-P-04.2. Specifically, the EPA did not ensure that POA&Ms had scheduled completion dates for milestone activities within the XACTA system. The EPA also did not review and update the POA&Ms monthly within the XACTA system to make sure that an accurate record existed of all planned, in-process, and completed actions to correct these deficiencies. Finally, the EPA did not provide support that it implemented adequate mitigating or compensating controls to address the risks associated with the 14 vulnerabilities remaining in the CDX, making the Agency more vulnerable to cyberattacks.

Specifically, we found that:

- The EPA's ability to track the status of all actions taken to correct these security weaknesses was hindered because the XACTA system did not have documentation of the CDX system owner's monthly reviews and updates of the POA&Ms for the 14 remaining vulnerabilities. EPA procedures require that the POA&Ms have milestone completion dates, yet the POA&Ms for these 14 remaining vulnerabilities did not. The system owner or other CDX system personnel assigns milestones to the POA&Ms to identify the required activities for full remediation of the vulnerability within a specified time frame. Often, there are multiple milestones within a POA&M, and each milestone must be detailed and include a completion date.

- A POA&M may be considered complete if the Agency accepts the risk. A system owner can submit a Risk Determination Waiver to request exemption from certain aspects of EPA information technology procedures. However, the Risk Determination Waiver should include (1) a detailed business justification and (2) information regarding implementation of compensating or mitigating controls.

  The Office of Information Security and Privacy rejected five Risk Determination Waiver requests for the CDX system. The Office of Information Security and Privacy waiver rejections stated that:

  > 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.

- Compliance with security requirements in a timely manner is necessary to protect against potential unauthorized disclosure or modification of CDX information, yet six of the 14 vulnerabilities had expired POA&M scheduled completion dates ranging from two weeks to 21 months.

Additionally, the EPA had deficiencies in validating the completion of POA&Ms for several vulnerabilities. The Agency did not adhere to the *POA&M Monitoring and Validation Standard Operating Procedure*, dated February 19, 2016, and the *XACTA POA&M Guide*, Version 5.0, dated October 2020. Specifically, the Agency closed a POA&M without having appropriate supporting security documentation in the XACTA system and did not review the security documentation submitted for POA&M closure in a timely manner. The system owner or other CDX system personnel are responsible for uploading security documentation into the XACTA system as evidence that the corrective actions were completed and that the underlying security control was operating efficiently. We found that:

- The CDX is potentially vulnerable to brute force attacks due to an unresolved password configuration vulnerability. Brute force attacks allow a threat actor to gain unauthorized access to an account by attempting multiple combinations of passwords. The Office of Information Security and Privacy prematurely closed a POA&M for a password configuration vulnerability without confirming that the POA&M's security documents supported and remediated the underlying vulnerability. The POA&M included documentation that a Risk Determination Waiver will be signed, but CDX system personnel failed to upload an approved and signed Risk Determination Waiver to support closing the POA&M.

- The Office of Information Security and Privacy is hindering the timely resolution of these vulnerabilities by failing to review these POA&Ms in a timely manner. It did not review and validate security documentation for two POA&Ms submitted by CDX system personnel for closure in June 2022 until June 2023, even though these POA&Ms were in a completed status and thus were required to be reviewed within a month. The *POA&M Monitoring and Validation Standard Operating Procedure* and *XACTA POA&M Guide* state that all corrective actions should be completed, and appropriate security documentation should be uploaded, to the XACTA system prior to a POA&M closure.

We identified a similar issue in OIG Report No. 23-E-0021, *The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently*, issued July 5, 2023. In that report, we recommended that the Agency (1) develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities and (2) assign responsibilities including documenting associated POA&Ms in the Agency tracking system. As of November 2023, these recommendations were resolved with corrective actions pending.[2]

According to the Cybersecurity and Infrastructure Security Agency, the time between a threat actor discovering a vulnerability and exploiting the vulnerability is decreasing. The Cybersecurity and Infrastructure Security Agency reported that, on average, threat actors exploit a vulnerability within 15 days of discovery. These 14 moderate- and high-risk vulnerabilities continue to remain in the CDX as of August 2023, 17 months after the independent assessor issued its March 2022 security assessment report. Left uncorrected, the EPA's network is more vulnerable to threat actors potentially exploiting these vulnerabilities and 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.

Agency Response and OIG Assessment

On September 19, 2023, the Office of Mission Support responded to our draft report, partially concurring with our findings. The Office of Mission Support stated that it believes that the Agency effectively manages the risks to the CDX and the EPA network. Further, it stated that the Agency uses software to monitor and track vulnerabilities through its POA&M process and that the CDX has compensating controls that reduce the risks of vulnerabilities being exploited. The Agency's response is attached to this report. At the EPA's request, we did not include the screenshots that the Agency attached to its response because of the sensitive nature of the content.

[2] We recommended that the assistant administrator for Mission Support develop a process to keep information security procedures consistent with the most current revision of the National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*. Additionally, we recommended that the assistant administrator for Air and Radiation develop, implement, and assign responsibilities for a plan to prioritize and schedule installation of patches that address critical vulnerabilities in the Analytical Radiation Data System within the Agency's required time frames.

The Agency's response had two overarching responses to our findings: (1) the Office of Mission Support stated that the CDX team reviews POA&Ms weekly and tracks the POA&M due dates in Jira, and (2) the Agency has compensating and mitigating controls that reduce the risks of vulnerabilities being exploited. However, we continue to find that CDX vulnerabilities were not tracked, monitored, and closed in compliance with the POA&M requirements identified in the Agency's *XACTA POA&M Guide*. The EPA established these requirements to track the resolution of vulnerabilities to better manage the risks to its systems. According to the *XACTA POA&M Guid*e, the XACTA system is the Agency's tool of record for managing the POA&M process. The XACTA system did not include documentation of the CDX system owner's monthly reviews and updates of the POA&Ms for the 14 unresolved vulnerabilities. Furthermore, the POA&Ms for these unresolved vulnerabilities did not include milestone completion dates in the XACTA system. The Agency's response acknowledges that information was not completely updated in the XACTA system and that POA&Ms may have expired completion dates. While the Agency provided Jira screenshots indicating that POA&Ms were in progress, on hold, or in a "to do" status, the Jira screenshots did not show that POA&Ms were updated monthly and that corrective actions were completed to resolve these vulnerabilities.[3]

While the Agency listed several compensating and mitigating controls within its response to our draft report, it did not provide any supporting documentation for these controls or describe how these controls address the risks associated with the 14 vulnerabilities remaining on the CDX system.[4] Further, as noted in our report, the Office of Information Security and Privacy rejected five Risk Determination Waivers submitted for the CDX that deviated from EPA policies and procedures because of a lack of compensating controls. The vulnerabilities remaining on the CDX 17 months after the issuance of the security assessment report leave the EPA's network susceptible to threat actors potentially exploiting these vulnerabilities.[5]

Additionally, the Agency's response raised concerns regarding specific terminology mentioned in the draft report. We reviewed the response and incorporated technical comments as appropriate.

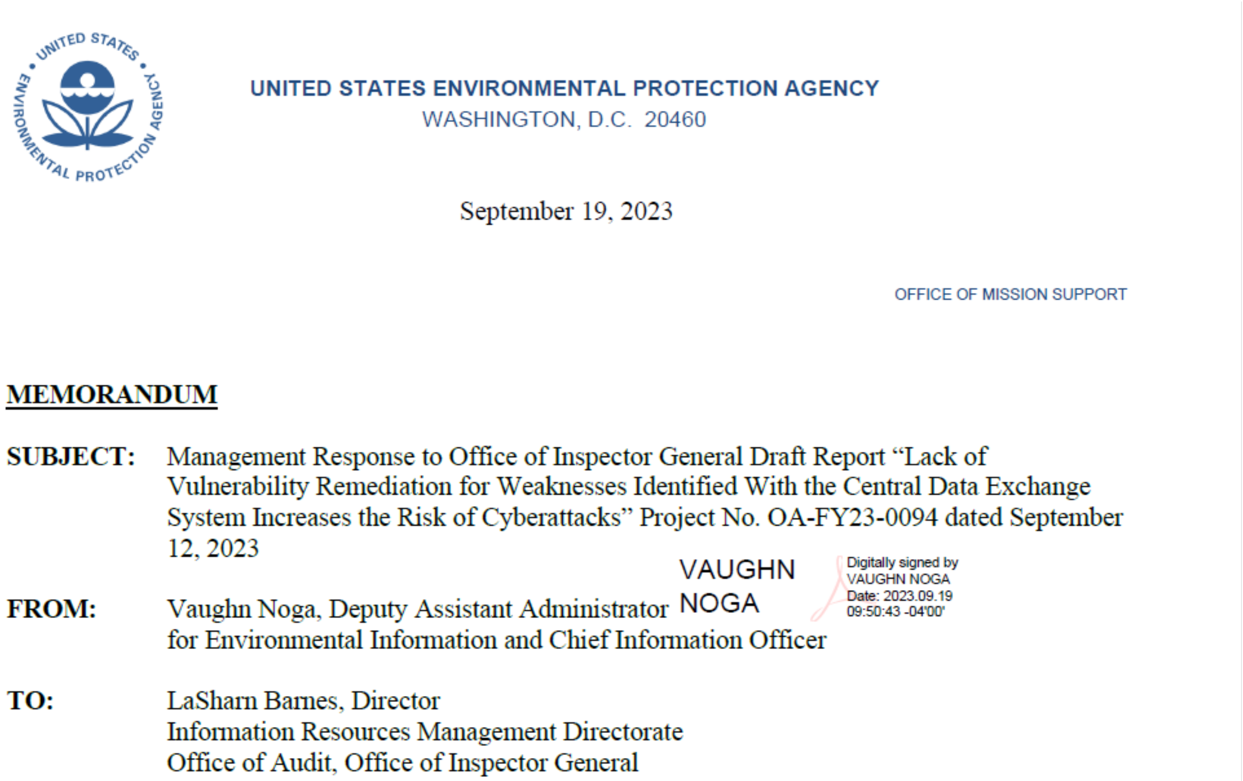
cc: Michael S. Regan, Administrator
Janet McCabe, Deputy Administrator
Dan Utech, Chief of Staff, Office of the Administrator
Wesley J. Carpenter, Deputy Chief of Staff for Management, Office of the Administrator
Faisal Amin, Agency Follow-Up Official (the CFO)
Andrew LeBlanc, Agency Follow-Up Coordinator
Susan Perkins, Agency Follow-Up Coordinator
Jeffrey Prieto, General Counsel
Tim Del Monico, Associate Administrator for Congressional and Intergovernmental Relations

[3] See attachment, "OMS Response To Report Concerns" table, No. 5, 6, 8, 9, 10, and 12.
[4] Any review of compensating or mitigating control documentation will be conducted during the overall audit.
[5] See attachment, "OMS Response To Report Concerns" table, No. 7, 11, 12, and 16.

Nick Conger, Associate Administrator for Public Affairs
Shari Grossarth, Office of Policy OIG Liaison
Stuart Miles-McLean, Office of Policy GAO Liaison
Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management, Office of Mission Support
Helena Wooden-Aguilar, Deputy Assistant Administrator for Workforce Solutions and Inclusive Excellence, Office of Mission Support
Dan Coogan, Deputy Assistant Administrator for Infrastructure and Extramural Resources, Office of Mission Support
Stefan Martiyan, Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Yulia Kalikhman, Acting Director, Office of Resources and Business Operations, Office of Mission Support
Tonya Manning, Director and Chief Information Security Officer, Office of Information Security and Privacy, Office of Mission Support
Michael Benton, Audit Follow-Up Coordinator, Office of the Administrator
Afreeka Wilson, Audit Follow-Up Coordinator, Office of Mission Support

Attachment A

Agency Response to Draft Report



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

September 19, 2023

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Management Response to Office of Inspector General Draft Report "Lack of Vulnerability Remediation for Weaknesses Identified With the Central Data Exchange System Increases the Risk of Cyberattacks" Project No. OA-FY23-0094 dated September 12, 2023

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

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.09.19 09:50:43 -04'00'

TO: LaSharn Barnes, Director
Information Resources Management Directorate
Office of Audit, Office of Inspector General

Thank you for the opportunity to respond to the concerns in the September 12th draft report titled "Lack of Vulnerability Remediation for Weaknesses Identified Within the Central Data Exchange System Increases the Risk of Cyberattacks" that outlined the OIG's concerns. Specifically, that:

1. "The EPA did not mitigate significant vulnerabilities identified on the CDX system;"
2. "These vulnerabilities increase the risk of threat actors gaining unauthorized access to CDX and its 49 interconnected systems;" and,
3. There are "deficiencies with validating the completion of the CDX plans of action and milestones, or POA&Ms, for several vulnerabilities."

Following is a summary of the agency's position on each of the concerns outlined in the report as well as additional context and information regarding the Central Data Exchange's (CDX) security posture. EPA believes that the agency effectively manages the risk to CDX and the EPA Network. For your consideration, we have also attached screen shots in the Appendix to supplement this response.

OMS RESPONSE TO REPORT CONCERNS

No.	OIG Concern or Statement	OMS' Response
1.	"The system allows end users to create accounts in CDX and provides identity verification services to gain access to 49 other environmental systems."	OMS does not concur. OMS does not understand how the OIG calculated "49 other environmental systems." CDX is comprised of human interactions and machine to machine interactions.
2.	*"The Central Data Exchange Security Assessment Report Continuous Monitoring Assessment – Year 2, dated March 2022, includes test results for the fiscal years 2020 through 2022 assessments. It identified 25 vulnerabilities associated with 21 security controls. Two of the 25 identified vulnerabilities were categorized as high risk,[2] while the remaining 23 were categorized as moderate risk.[3]"*	Concur with the statement, however, OMS does not concur with the implications that it provides further in the report. The Assessment report had 25 findings related to the controls. This resulted in 18 POA&Ms of which 6 have been closed (including one of the two identified high risk vulnerabilities); remaining are 1 Agency level, 7 relate to ICAM; 4 CDX specific. Plans of Actions and Milestones (POA&Ms) are a risk management process that provides increased security awareness of vulnerabilities and enables the agency to enact a stronger security posture on systems, including mitigating controls. POA&Ms will be created at any point a vulnerability is identified and CIO 2150-P-04.2 CA-5 (1) (a) (i) – lists how POA&Ms can be identified. CDX is constantly monitoring and addressing security vulnerabilities during that same timeframe between October 1, 2019 and September 30, 2022 CDX closed 112 POA&Ms. While this audit has been underway, CDX has also opened an additional 8 POA&Ms, of which 2 have also been closed. The most current version of the XACTA POA&M Guide is 5.1, dated October 2020.
3.	*"National Institute of Standards and Technology Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, dated December 2018, states that system owners prepare CDX POA&Ms based on the findings and recommendations of the security assessment reports."*	Typo. "…states that system owners prepare CDX POA&Ms…" NIST reference to CDX.

4.	*"The purpose of these POA&Ms is to 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."*	Plans of Actions and Milestones (POA&Ms) are a risk management process that provides increased security awareness of vulnerabilities and enables the agency to enact a stronger security posture on systems, including mitigating controls. POA&Ms will be created at any point a vulnerability is identified and CIO 2150-P-04.2 CA-5 (1) (a) (i) – lists how POA&Ms can be identified. The most current version of the XACTA POA&M Guide is 5.1, dated October 2020.
5.	*"The EPA did not ensure POA&Ms had scheduled completion dates for milestone activities."*	Do not concur. CDX tracks POA&M due dates in Jira and POA&Ms are reviewed weekly by the CDX security team (see Appendix screen shots).
6.	*"The EPA also did not review and update the POA&Ms monthly to make sure that an accurate record of all planned, in process, and completed actions existed to correct these deficiencies."*	Do not concur. The CDX team does review POA&Ms weekly in Jira (see Appendix attached screenshots).
7.	*…"the EPA did not implement adequate mitigating or compensating controls to address the risks associated with these 14 vulnerabilities remaining on the CDX system, making the Agency more vulnerable to cyberattacks."*	Do not concur. CDX has implemented several security layers of compensating controls, for example: • Network Security Groups (NSG): to prevent unauthorized network route access. • Key Vault: Credentials are stored in a secured location versus packaged with the applications. SSL certificates are also stored in a key vault so threat actors are unable to masquerade as a CDX resource. • Defender for Cloud; Defender for Servers; Defender for Containers; Defender for Open Source Databases: Cloud native security tools that provide (dashboard) near real time security posture for CDX resources. • Splunk integration: CDX has integrated with the Agency log warehouse.
8.	*EPA did not ensure POA&Ms had scheduled completion dates for milestone activities.*	Do not concur. See above.

9.	*“The EPA’s ability to track the status of all actions taken to correct these security weaknesses was hindered because the Agency’s Information Security Repository system did not have documentation of the CDX system owner’s monthly reviews and updates of the POA&Ms for the 14 remaining vulnerabilities.”*	Do not concur. CDX does track actions taken in Agency tools, and regularly updates actions in Jira, but acknowledges the information was not completely entered into XACTA.
10.	*“EPA procedures require that the POA&Ms have milestone completion dates, yet the POA&Ms for these 14 remaining vulnerabilities did not. The system owner or CDX system personnel assigns milestones to the POA&Ms to identify the required activities for full remediation of the vulnerability within a specified time frame. Often, there are multiple milestones within a POA&M, and each milestone must be detailed and include a completion date.”*	Same as above.
11.	*“The Office of Information Security and Privacy rejected five Risk Determination Waiver requests for the CDX system because the waivers did not include a business justification and compensating or mitigating controls to reduce the risk from the system’s deviation from existing EPA policies and procedures.”*	Do not concur. Although these 5 Risk Determination Waivers were rejected it was not because a business justification was not provided. Currently, a Risk Determination Request can be submitted without including compensating or mitigating controls.
12.	*“Timely compliance with security requirements are necessary to, among other things, protect against potential unauthorized disclosure or modification of CDX information; yet, six of the 14 vulnerabilities had expired POA&M scheduled completion dates ranging from two weeks to 21 months.”*	Concur that Timely compliance with security requirements are necessary and that POA&Ms may have expired completion dates in XACTA. However, CDX has implemented many layers of compensating controls to reduce vulnerabilities being exploited.
13.	*“The CDX system continues to remain vulnerable to brute force attacks, which would allow a threat actor to gain unauthorized access to an account by guessing the password by attempting multiple combinations of passwords.”*	Do not concur. EPA has several mechanisms in place to detect and prevent brute force attacks. Specifically, CDX has more stringent controls than Agency procedures (CIO 2150-P-01.3) implemented on the system to lock accounts after 3 unsuccessful attempts (versus 5 per agency policy).
	“The Office of Information Security and Privacy is hindering the timely resolution of these vulnerabilities by failing to review these POA&Ms for 12 months. The Agency did not review and validate security	Concur however the referenced procedure is not the latest document for POA&M Monitoring and Validation. The link enclosed provides the current guidance.

14.	*documentation for two POA&Ms submitted by CDX system personnel for closure in June 2022 until June 2023 when the Office of Information Security and Privacy reviewed and updated the status of these POA&Ms. The POA&M Monitoring and Validation Standard Operating Procedure states that all corrective actions should be completed and appropriate security documentation is uploaded to the Agency Information Security Repository system prior to a POA&M closure."*	https://usepa.sharepoint.com/:w:/s/oei_Community/OISP/ERHzftywr51Fr9V-FPe8hOABSuenwHEDcYs6xvXlYF4zsw
15.	*"Furthermore, we identified a similar issue in OIG Report No. 23-E-0021, The EPA's Vulnerability Tracking and Remediation and Information Technology Procedures Review Processes Are Implemented Inconsistently, issued July 5, 2023. In that report, we recommended that the Agency* (1) *develop and implement a plan for prioritizing and scheduling the installation of patches that address vulnerabilities and* (2) *assign responsibilities including documenting associated POA&Ms in the Agency tracking system. These recommendations were resolved with corrective actions pending."*	Do not concur. OISP has implemented procedures to address the two recommendations With respect to item #1 the Information Security – Interim System and Information Integrity Procedures (Control SI-2 – Flaw Remediation, Item 2(b)) states that System Owners (SO) in coordination with others "Prioritize vulnerabilities and remediation actions based on the individual vulnerability criticality or severity ratings". With respect to item #2 the same procedure (Section 7 – Roles and Responsibilities) assigns responsibility to the System Owner (SO) "Manage and report flaw remediation to the SAISO through the POA&M process via the Agency's FISMA reporting and tracking tool." (sub-item 'g').
16.	*Left uncorrected, the EPA's network is more vulnerable to threat actors exploiting these vulnerabilities and gaining access to the CDX system and the environmental data relied upon by states, tribes, and other entities, as well as potential disclosure and modification of data for the 49 systems that are interconnected to the CDX system."*	Do not concur. EPA has implemented numerous mitigating controls for these 14 vulnerabilities and is monitoring and tracking these vulnerabilities through the POA&M process. CDX has deployed cloud native tools that allow near real time remediation of vulnerabilities and are maturing our operations of these tools. Additionally, CDX's Software Development Life Cycle (SDLC) processes are evolving and increasing

		cross collaboration throughout the delivery lifecycle to respond more quickly to findings/vulnerabilities.

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.

Attachment: Technical Materials

Cc: Tertia Allen
Yoon An
Troy Givens
Nii-Lantei Lamptey
Iantha Maness
Christina Nelson
Teresa Richardson
Scott Sammons
Michelle Wiker
Erin Collard
Austin Henderson
David Alvarado
Jennie Campbell
Dwane Young
Joe Carioti
Tonya Manning
Mark Bacharach
Dan Coogan
Marilyn Armstrong
Susan Perkins
OMS_Audit_Coordination@epa.gov

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

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 Inquiries: OIG.CongressionalAffairs@epa.gov

Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X (formerly Twitter): @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov