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

OFFICE OF
INSPECTOR GENERAL

April 21, 2023

MEMORANDUM

SUBJECT: Notification of Audit:
The EPA's Compliance with the Federal Information Security Modernization Act for FY 2023
Project No. OA-FY23-0061

FROM: LaSharn Barnes, Director
LASHARN BARNES
Digitally signed by LASHARN BARNES
Date: 2023.04.21 11:46:24 -04'00'
Information Resources Management Directorate
Office of Audit

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

Radhika Fox, Assistant Administrator
Office of Water

The U.S. Environmental Protection Agency Office of Inspector General plans to begin an audit of the EPA's compliance with the Federal Information Security Modernization Act of 2014. This audit is statutorily required and is part of the OIG's oversight plan for fiscal year 2023. This audit also addresses the following fiscal year 2023 top management challenge for the Agency: protecting EPA systems and other critical infrastructure against cyberthreats.

Our objective is to assess the EPA's compliance with the *Office of Management and Budget's Fiscal Year 2023 Inspector General FISMA Reporting Metrics*. We plan to conduct work within the Office of Mission Support and the Office of Water at EPA headquarters. We will use applicable generally accepted government auditing standards to conduct our audit. The anticipated benefit of the audit is to meet the congressional mandate by assessing the Agency's information security program against fiscal year 2023 FISMA requirements.

We will contact you to arrange a mutually agreeable time to discuss our objective. At that time, we can discuss any concerns that you may have and answer any questions about the audit process, reporting procedures, methods used to gather and analyze data, and what we should expect of each other during the audit. Throughout the audit, we will provide updates on a regular basis.

To expedite our audit, please be ready to provide the information listed in our initial documentation request, which include the corresponding FISMA metric numbers and responsible offices (Attachment A). These requests relate to the Agency's information technology processes and the Safe Drinking Water Information System.

We respectfully note that the Inspector General Act of 1978, as amended, authorizes the OIG to have timely access to personnel and all materials necessary to complete its objectives. Similarly, EPA Manual

6500, *Functions and Activities of the Office of Inspector General* (1994), requires that each EPA employee cooperate with and fully disclose information to the OIG. Also, Administrator Michael S. Regan, in an April 28, 2021 email message to EPA employees, conveyed his "expectation that EPA personnel provide OIG timely access to records or other information" and observed that "full cooperation with the OIG is in the best interest of the public we serve." If an Agency employee or contractor refuses to provide requested materials to the OIG or otherwise fails to cooperate with the OIG, we will request that you immediately resolve the situation. Consistent with the IG Act, we may report unresolved access matters to the administrator and to Congress.

We will post this memorandum on our public website at www.epa.gov/oig. Anyone with knowledge of potential fraud, waste, abuse, misconduct, or mismanagement related to this audit should contact the OIG Hotline at (888) 546-8740 or via an electronic form on the "OIG Hotline" webpage.

Attachment

cc: Janet McCabe, Deputy Administrator
Dan Utech, Chief of Staff, Office of the Administrator
Jon Monger, Assistant Deputy Administrator
Wesley J. Carpenter, Deputy Chief of Staff for Management, Office of the Administrator
Andrew Schreyer, Deputy Assistant Administrator for Mission Support
Vaughn Noga, Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Benita Best-Wong, Deputy Assistant Administrator for Water
Bruno Pigott, Deputy Assistant Administrator for Water
Dan Coogan, 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 Policy, Office of Mission Support
Macara Lousberg, Director, Office of Program Analysis, Regulatory, and Management Support, Office of Water
Janita Aguirre, Associate Director, Office of Program Analysis, Regulatory, and Management Support, Office of Water
Robert Kelly, Acting Branch Chief, Office of Information Security and Privacy, Training, Compliance, and Oversight, Office of Mission Support
Afreeka Wilson, Audit Follow-Up Coordinator, Office of Mission Support
Cameo Smoot, Audit Follow-up Coordinator, Office of Water
Susan Perkins, Agency Follow-Up Coordinator
Andrew LeBlanc, Agency Follow-Up Coordinator
José Kercado, Agency Follow-Up Coordinator
Marie Michalos, Acting Associate Administrator for Public Affairs
Lance McCluney, Director, Office of Administrative and Executive Services, Office of the Administrator
Regional Audit Follow-Up Coordinators, Regions 1–10
Sean W. O'Donnell, Inspector General
Nicole N. Murley, Acting Deputy Inspector General

Attachment A

Request #	IG FISMA Metric #	IG FISMA Domain	Request Description	Related Process/Tool	Responsible Office	OIG POC	Question on this request related to OMS Enterprise Tool listing response
1	1	Risk Management	Listing of all EPA information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections.	Xacta	OISP	LaVonda Harris-Claggett	Is there an Xacta report that would produce a comprehensive and accurate inventory of all EPA information systems?
2	1	Risk Management	EPA's inventory of the software and associated licenses	Xacta	OISP		In response to Rec #1 of OIG Report No. 20-P-0120, OMS completed an asset inventory in 2020. Additionally, EAMS records show corrective actions to develop and deploy an enterprise Software Asset and Configuration Management (SACM) capability that aligns license entitlement data with software inventories was completed 9/29/22. Is this accurate?
3	2	Risk Management	EPA's authorized hardware inventory list containing identifying information for a device, when it was authorized, when the authorization expires, who manages the device and the removable media authorized for each device		OISP	LaVonda Harris-Claggett	Does EPA maintain a centralized hardware inventory listing?
4	2	Risk Management	Inventory of information system components as described in the Interim Configuration Mangement Procedures, CIO 2150.3-P-05.1, Control CM-8a (page 11 of 25), which states "an inventory of information system components or CIs that accurately reflects the current information system must be developed, documented, and maintained", if different than listing provided for Requests #1-3 above.		OISP	LaVonda Harris-Claggett	
5	2	Risk Management	Latest Continuous Monitoring Report (Vulnerability Scan Report) for the EPA network		OISP	LaVonda Harris-Claggett	
6	2	Risk Management	Listing of unauthorized hardware discovered by EPA (which includes servers, mobile devices, endpoints, and network devices)		OISP	LaVonda Harris-Claggett	
7	2	Risk Management	Documented procedures addressing the development and maintenance of an inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information necessary for tracking and reporting.	IT procedures	OISP	LaVonda Harris-Claggett	
8	2	Risk Management	Listing of SDWIS Incident tickets between 10/1/2022 and present		OW OISP SOCD	LaVonda Harris-Claggett	
9	2	Risk Management	Enterprise Architecture documents		OISP	LaVonda Harris-Claggett	

	Population Request
	Procedures Request

10	2	Risk Management	Inventory dashboards for SDWIS		OW	LaVonda Harris-Claggett	
11	2	Risk Management	Firewall configurations/logs for SDWIS		OW	LaVonda Harris-Claggett	
12	3	Risk Management	Documented procedures addressing the development and maintenance of an inventory of software and associated licenses used within the organization with the detailed information necessary for tracking and reporting.	IT Procedures	OISP	LaVonda Harris-Claggett	
13	5	Risk Management	3 Most Recent Risk Assessment Reports for SDWIS		OW	LaVonda Harris-Claggett	
14	5	Risk Management	Documentation of EPAs Risk Management Strategic Plan that describes the Enterprise Risk Management Process (ERMP)	IT Procedures	OISP	LaVonda Harris-Claggett	
15	5	Risk Management	System Security Plan for SDWIS (if one exists dated later than 3/1/2022).		OW	LaVonda Harris-Claggett	We've downloaded the March 1, 2022 version off Xacta. This request is to confirm we have the latest version.
16	7	Risk Management	Documentation addressing the relationship between cybersecurity risk management roles and those roles involved with enterprise risk management.	IT Procedures	OISP	LaVonda Harris-Claggett	
17	7	Risk Management	Documentation addressing the Risk Management Framework role assignments	IT Procedures	OISP	LaVonda Harris-Claggett	
18	7	Risk Management	Office of Water (OW) Organizational Chart that shows responsibility over the SDWIS system		OW	LaVonda Harris-Claggett	
19	7	Risk Management	Documented procedures on the use of cybersecurity risk registers which help record the progress of management processes	IT Procedures	OISP	LaVonda Harris-Claggett	
20	8	Risk Management	Documentation to support what methods are used to communicate SDWIS risk to stakeholders	IT procedures	OISP	LaVonda Harris-Claggett	
21	8	Risk Management	Listing of system level POA&Ms for SDWIS tracking the findings from the security and privacy assessment reports that are to be remediated.	Xacta	OW	LaVonda Harris-Claggett	
22	8	Risk Management	Listing of POA&Ms across all EPA systems.	Xacta	OISP	LaVonda Harris-Claggett	Can Xacta produce a population of POA&Ms across all EPA system?
23	9	Risk Management	The last two cybersecurity risk communications from OISP to the EPA community.		OISP	LaVonda Harris-Claggett	What are OISP's methods for communicating and sharing with the EPA community on cyber risk? Where do you store those communications with the EPA community?

24	10	Risk Management	Documentation addressing cybersecurity risk dependencies, risk scores/levels, and management dashboards to address the automated enterprise wide view of cybersecurity risk activities.	IT Procedures	OISP	LaVonda Harris-Claggett	
25	12	Supply Chain Risk Management	Supply Chain Risk Management Policy and Procedures documentation and evidence of its communication to relevant staff (if not posted on the intranet)	IT procedures	OISP (in coordination with OAS)	Gina Ross	
26	12	Supply Chain Risk Management	Agencywide Supply Chain Risk Management Strategy		OISP (in coordination with OAS)	Gina Ross	
27	13	Supply Chain Risk Management	Documentation of most recent lessons learned conducted to review and update its SCRM policies, procedures, and processes.		OISP (in coordination with OAS)	Gina Ross	
28	14	Supply Chain Risk Management	Listing of contracts related to the SDWIS -Contract for operation of the system - RFP for the system - Documentation of Agency review of acquisition package (Response to RFP)		OW	Gina Ross	
29	14	Supply Chain Risk Management	Test Result or Report of evaluation performed on suppliers to determine adherence to security or SCRM requirements for SDWIS		OW	Gina Ross	
30	14	Supply Chain Risk Management	Copy of the cybersecurity checklist included in all acquisition contracts		OISP (in coordination with OAS)	Gina Ross	
31	14	Supply Chain Risk Management	Listing of information security contracts to include those related to products, system components, systems, and services of external providers.		OISP (in coordination with OAS)	Gina Ross	
32	19	Configuration Management	Inventory of information system components for SDIWS		OW	Shah Qureshi	
33	19	Configuration Management	Last 2 baseline configurations for SDWIS		OW	Shah Qureshi	
34	20	Configuration Management	Last public vulnerability disclosure on SDWIS for FY22		OW	Shah Qureshi	
35	21	Configuration Management	System generated evidence showing SDWIS database version		OW	Shah Qureshi	
36	21	Configuration Management	SDWIS Patch History for FY22		OW	Shah Qureshi	

37	22	Configuration Management	Documented procedures related to EPA's plan to meet the goals of the TIC initiative, consistent with OMB M-19-26. Specifically, the agency has defined and customized procedures and processes to implement TIC 3.0, including updating its network and system boundary policies, in accordance with OMB M-19-26.	IT procedures	OISP OITO	Shah Qureshi	
38	22	Configuration Management	Documentation supporting implementation of TIC use cases in accordance with OMB M-19-26.		OISP OITO	Shah Qureshi	
39	22	Configuration Management	Documented procedures related to EPA's development and maintenance of an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection.	IT procedures	OISP OITO	Shah Qureshi	
40	24	Configuration Management	Listing of internet-accessible systems utlizing the Agency's vulnerability disclosure policy.		OISP	Shah Qureshi	
41	24	Configuration Management	Documented vulnerability disclosure handling procedures to support the implementation of its VDP.	IT procedures	OISP	Shah Qureshi	
42	29	Identity Credential and Access Management	Name of the system that captures and stores all the "National Rules of Behavior (NROB)"	Xacta	OISP	Eric Jackson	What's the process for reporting on individuals that didn't sign the NROB? Is there a system generated report?
43	30	Identity Credential and Access Management	System generated listing of SDWIS users to include Name, Access Type, username, account creation date, account status. (Please included the system script use to pull the data)		OW	Eric Jackson	
44	30	Identity Credential and Access Management	System generated listing of SDWIS users with access to modify or delete data. (Please included the system script use to pull the data)		OW	Eric Jackson	
45	32	Identity Credential and Access Management	Most recent system log that captures the following SDWIS activities: Privileged system access, and Privileged command execution. (Please ensure the logs captures timestamps such as date and time, identified user and actions)		OW	Eric Jackson	
46	33	Identity Credential and Access Management	Screen shot of the SDWIS configuration setting for remote access connection sessions time out feature.		OW	Eric Jackson	
47	35	Data Privacy	Documentation of privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed of by its information systems.	IT procedures	OISP NPP	Sabrena Richardson	

48	35	Data Privacy	Documentation of the roles and responsibilities for the effective implementation of the organization's privacy program to include the resources and optimal governance structure needed to effectively implement its privacy program.	IT procedures	OISP NPP	Sabrena Richardson	
49	36	Data Privacy	Most recent continuous monitoring assessment for SDWIS		OW	Sabrena Richardson	
50	36	Data Privacy	Screenshots of SDWIS configuration settings that support access controls or methods used to prevent and detect untrusted removable media.		OW	Sabrena Richardson	
51	36	Data Privacy	Evidence of exercises testing SDWIS access controls that pertain to removable media, destruction, and sanitation of media.		OW	Sabrena Richardson	
52	36	Data Privacy	Most recent listing of disposed media for SDWIS		OW	Sabrena Richardson	
53	36	Data Privacy	SDWIS system documentation addressing workflow, system designs and operation flowcharts used to prevent data breaches.		OW	Sabrena Richardson	
54	37	Data Privacy	Screen shots of SDWIS configuration settings that describe : web content filters, reports associated with capturing monitoring of inbound and outbound network traffic for phishing, malware, and domain filtering (A meeting can be scheduled to walkthrough these settings to demonstrate)		OW	Sabrena Richardson	
55	37	Data Privacy	SDWIS DNS record audit results for the last 2 quarters		OW	Sabrena Richardson	
56	37	Data Privacy	Evidence of SDWIS domain encryption certificates.		OW	Sabrena Richardson	
57	42	Security Training	EPA's Enterprise Cybersecurity training program documentation that identifying roles that require focused, specialized training.	FedTalent	OISP	Gina Ross	
58	43	Security Training	Security Awareness Training Plan, to include: •EPA Annual Report on Cyber Work Roles Action Plan Update •ISO and ISSO Action Plan •IT PM Action Plan •Agency Plan to Address Cyber security work roles of critical need •EPA Annual Report on Cyber Work Roles of Critical Need		OISP	Gina Ross	
59	47	Information System Conituous Monitoring	Latest Continuous Monitoring Report (Vulnerability Scan Report) for SDWIS.		OW	Eric Jackson	
60	47	Information System Conituous Monitoring	Dashboard screenshot for SDWIS showing vulnerabilities or capability to capture vulnerabilities status (if different from continuous monitoring report request above).		OW	Eric Jackson	

61	49	Information System Conituous Monitoring	Listing of the SDWIS POA&Ms for the last 2 quarters.	Xacta	OW	Eric Jackson	
62	49	Information System Conituous Monitoring	SDWIS ATO letters - most recent current and previous	Xacta	OW	Eric Jackson	
63	49	Information System Conituous Monitoring	Most recent SDWIS security assessment report (SAR) (to include any third party security assessment).	Xacta	OW	Eric Jackson	
64	54	Incident Response	Screen Shots of SDWIS system configurations that capture security controls to prevent data exfiltration and network defenses		OW	Shah Qureshi	
65	54	Incident Response	Last 2 lessons learned performed on the effectiveness of SDWIS's incident detection policies and procedures.		OW	Shah Qureshi	
66	55	Incident Response	Population listing of incident tickets across all EPA systems for 10/1/2022 and present		OISP SOCD	Shah Qureshi	
67	55	Incident Response	Documented procedures for incident handling, which includes the strategies for each key incident types and a process to eradicate components of an incident, mitigate any vulnerabilities that were exploited	IT procedures	OISP SOCD	Shah Qureshi	
68	57	Incident Response	Documented procedures for collaboration with DHS and other parties, to include use DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's Networks	IT procedures	OISP SOCD	Shah Qureshi	
69	57	Incident Response	Listing of all Region and Program Office Information Management Officers.		OISP	Shah Qureshi	
70	57	Incident Response	Listing of contractual relationships in support of Incident Response Process (ie, MOUs, emails, etc)		OISP (in coordination with OAS)	Shah Qureshi	
71	57	Incident Response	Documentation of usage of DHS' Einstein 1 and 2 for screening of traffic into and out of the EPA network for SDWIS		OISP SOCD OW	Shah Qureshi	
72	58	Incident Response	Documented procedures for providing the information about the web application protections, event and incident management (such as intrusion detection and prevention tools, and incident tracking and reporting tools), aggregation and analysis (such as security information and event management (SIEM) products), information management (such as data loss prevention), and file integrity and endpoint and server security tools.	IT procedures	OISP SOCD	Shah Qureshi	

73	58	Incident Response	Any SOPs or documentation related to SDWIS' access management (if different from Agencywide Access Control procedures)	IT procedures	OW	Shah Qureshi	
74	58	Incident Response	SDWIS' hardware inventory listing		OW	Shah Qureshi	
75	58	Incident Response	Zero Tust Implementation Plan and budget		OISP SOCD	Shah Qureshi	
76	58	Incident Response	Name of the EPA's Zero Trust Strategy implementation lead		OISP SOCD	Shah Qureshi	
77	58	Incident Response	Documentation on the ISCM strategy encompassing technology, processes, procedures, operating environments, and people.		OISP SOCD	Shah Qureshi	
78	60	Contingency Planning	Documentation of Test, Training, and Exercise (TT&E) program reports showing IT personnel training reports for their roles and responsibilities for SDWIS		OW	Sabrena Richardson	
79	60	Contingency Planning	Documentation of the most recent Risk Management Cycle report for SDWIS		OW	Sabrena Richardson	
80	61	Contingency Planning	Documentation of the last 3 Business Impact Analysis reports identifying potential impacts on the performance of essential functions and consequences of failure to sustain them for SDWIS		OW	Sabrena Richardson	
81	61	Contingency Planning	Documentation of criticality analysis report that identifies critical system components and functions for SDWIS		OW	Sabrena Richardson	
82	63	Contingency Planning	Documentation of the last 3 Information System Contingency Plan testing reports for SDWIS		OW	Sabrena Richardson	
83	63	Contingency Planning	Documentation of the last 2 After action reports for SDWIS		OW	Sabrena Richardson	
84	65	Contingency Planning	Documentation of the last 3 Incident handling reports for SDWIS		OW	Sabrena Richardson	
85	65	Contingency Planning	Documentation to support communication of the last 3 recovery activites/reports that were communicated to internal and external stakeholders/ executive/management teams for SDWIS		OW	Sabrena Richardson	