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

OFFICE OF
INSPECTOR GENERAL

December 15, 2020

MEMORANDUM

SUBJECT: Notification of Audit:
Follow-Up on Prior OIG Cybersecurity Audit Recommendations
Project No. OA-FY21-0067

FROM: Rudolph M. Brevard, Director Rudolph M. Brevard
Information Resources Management Directorate
Office of Audit

TO: David Bloom, Deputy Chief Financial Officer

Alexandra Dapolito Dunn, Assistant Administrator
Office of Chemical Safety and Pollution Prevention

Peter Wright, Assistant Administrator
Office of Land and Emergency Management

Donna Vizian, Principal Deputy Assistant Administrator
Office of Mission Support

The Office of Inspector General for the U.S. Environmental Protection Agency plans to begin the subject audit. This audit is self-initiated and addresses the following top management challenges for the Agency, as identified in our *EPA's FYs 2020–2021 Top Management Challenges* report, issued July 21, 2020:

- Complying with key internal control requirements (data quality; policies and procedures).
- Enhancing information technology security.

The OIG's objectives are to determine whether:

1. The EPA completed corrective actions for agreed-to cybersecurity audit recommendations in OIG reports issued from fiscal years 2017 through 2020.
2. The actions taken by the EPA effectively resolved the weaknesses identified in select audit reports.

The OIG plans to conduct work at EPA headquarters and other regional offices, as needed. Applicable generally accepted government auditing standards will be used in conducting our audit. The anticipated benefits of this audit are to improve and strengthen the EPA's internal controls to correct IT security deficiencies identified in OIG reports.

We will contact you to arrange a mutually agreeable time to discuss our objectives. We would also be particularly interested in any areas of concern that you may have. We will answer any of your 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.

We have attached a list of reports that we will be following up on. The list includes the reports' recommendations and associated corrective actions whose completion dates have passed. To expedite our audit, please provide documentation supporting the completion of each of the Agency's proposed corrective actions listed in the attachment at the entrance conference.

We respectfully note that the OIG is authorized by the Inspector General Act of 1978, as amended, to have timely access to personnel and all materials necessary to complete its objectives. We will request that you immediately resolve the situation if an Agency employee or contractor refuses to provide requested materials to the OIG or otherwise fails to cooperate with the OIG. We may report unresolved access matters to the administrator and include the incident in the *Semiannual Report to Congress*.

I will supervise the audit, and the team lead will be Jeremy Sigel. Any information related to the audit should be addressed to Jeremy Sigel at (202) 566-0852 or sigel.jeremy@epa.gov or to me at (202) 566-0893 or brevard.rudy@epa.gov.

Attachment

cc: Henry Darwin, Assistant Deputy Administrator
Doug Benevento, Associate Deputy Administrator
Mandy Gunasekara, Chief of Staff
Michael Molina, Deputy Chief of Staff/Operations
Wesley J. Carpenter, Acting Deputy Chief of Staff
Carol Terris, Associate Chief Financial Officer
Paige Hanson, Associate Chief Financial Officer for Policy
Jeanne Conklin, Controller
Meshell Jones-Peeler, Deputy Controller
Aileen Atcherson, Director, Policy, Training, and Accountability Divison, Office of the Controller
Nikki Newton, Branch Chief, Management, Integrity and Accountability Branch; Policy Training, and Accountability Divison, Office of the Controller
Nancy Beck, Principal Deputy Assistant Administrator for Chemical Safety and Pollution Prevention
David Fischer, Deputy Assistant Administrator for Chemical Safety and Pollution Prevention
Barry Breen, Principal Deputy Assistant Administrator for Land and Emergency Management
Steven Cook, Deputy Assistant Administrator for Land and Emergency Management
David Zeckman, Associate Deputy Assistant Administrator for Mission Support
Dan Coogan, Acting Director, Office of Resources and Business Operations, Office of Mission Support
Vaughn Noga, Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Andrew LeBlanc, Agency Follow-Up Coordinator
José Kercado, Backup Agency Follow-Up Coordinator

Janet Weiner, Audit Follow-Up Coordinator, Office of Chemical Safety and Pollution Prevention
Kecia Thornton, Audit Follow-Up Coordinator, Office of Land and Emergency Management
Mitchell Hauser, Audit Follow-Up Coordinator, Office of Mission Support
James Hewitt, 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
Charles J. Sheehan, Deputy Inspector General
Edward S. Shields, Associate Deputy Inspector General
Eric W. Hanger, Acting Counsel to the Inspector General
Benjamin May, Chief of Staff
Katherine Trimble, Assistant Inspector General for Audit
Rashmi Bartlett, Acting Assistant Inspector General for Evaluation
Helina P. Wong, Assistant Inspector General for Investigations
Stephanie L. Wright, Assistant Inspector General for Management
Christine El-Zoghbi, Deputy Assistant Inspector General for Evaluation
James Hatfield, Associate Deputy Assistant Inspector General for Audit
Richard J. Eyermann, Director, Mission Support Directorate, Office of Audit, Office of Inspector General
Jennifer Kaplan, Deputy Assistant Inspector General for Congressional and Public Affairs
Jeffrey Lagda, Congressional and Media Liaison, Office of Inspector General

Attachment

Report Number, name and date	Recommendation	Corrective Action	Original completion date
17-P-0029, Acquisition Certifications Needed for Managers Overseeing Development of EPA's Electronic Manifest System, November 7, 2016	We recommend that the **assistant administrator for Land and Emergency Management:** 2. Implement internal controls to enforce the requirement that the e-Manifest system program and project managers obtain the Federal Acquisition Certification for Program and Project Managers – Information Technology specialized certification once the Agency issues the new EPA Federal Acquisition Certification for Program and Project Managers program guidance.	The Office of Resource Conservation and Recovery will amend the position descriptions of personnel covered by the OIG's recommendation to reflect the requirement for the Federal Acquisition Certification for Program and Project Managers – Information Technology. In addition, the ORCR will add this requirement as a performance measure to the Performance Appraisal and Recognition System Performance Standards of covered personnel. This will allow the ORCR to conduct a midyear and yearly evaluation of compliance with the certification requirements of the guidance. The ORCR commits to add this requirement to pertinent performance agreements that will be put in place for FY 2017. Lastly, the ORCR will submit revised position descriptions for covered personnel to the Office of Administration and Resource Management by December 2016.	12/30/16
17-P-0344, EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection, July 31, 2017	We recommend that the **assistant administrator for Administration and Resources Management:*** 1. Update the EPA Acquisition Guide to include cybersecurity tasks contained in Interim Policy Notice # 17-01, Use of 22 Cybersecurity Tasks (December 2016).	The Office of Acquisition Management does not feel comfortable setting any date for this Interim Policy Notice # 17- 01 – Use of 22 Cybersecurity Tasks (December 2016) because this is really an OMB initiative. The EPA, in being proactive, developed and prepared the IPN as official Agency acquisition policy to be followed. With that said, an estimated milestone date would be October 31, 2019. This is contingent upon the: 1) use of the tasks in solicitations and the receipt of feedback from the vendor communities and 2) the OMB's release of cybersecurity clauses via FAR (FAC-xx).	10/31/19
	We recommend that the **assistant administrator for Environmental Information* and chief information officer:** 3. Work with the assistant administrator for Administration and Resources Management to implement a process that requires appropriate Agency personnel to maintain a	The Office of Environmental Information agrees with the revised recommendation, with a few clarifications. First, it asked that the recommendation be changed from "Implement a process" to state that "OEI will work with the Assistant Administrator for Administration and Resources Management (OARM) to implement a	12/31/18

	listing of contractor personnel who have significant information security responsibilities and are required to take role-based training. This process should require appropriate Agency personnel to validate and report to the chief information security officer that all relevant contractor personnel have completed role-based training.	process." This may require actions from contracting officer representatives and would necessitate coordination with the OARM. Second, OEI would attest that Agency personnel should respond to the chief information security officer, not the senior agency information security officer, that all relevant contractor personnel have completed role-based training.	
	4. Include the number of contractors who have significant information security responsibilities and have completed the required role-based training in the Chief Information Officer's Annual Federal Information Security Modernization Act reports submitted to the Office of Management and Budget.	The OEI agrees in part that based upon a recent change in A-130, Appendix I, this requirement can be met by the end of FY 2017.	9/30/17
18-P-0298, Management Alert: EPA's Incident Tracking System Lacks Required Controls to Protect Personal Information, September 28, 2018	We recommend that the **assistant administrator for Environmental Information**:* 1. Develop and implement a strategy that protects the confidentiality of personally identifiable information and sensitive personally identifiable information, as required by federal and EPA privacy and password guidance, for incident tickets in the current incident tracking system.	Implement a strategy to redact personally identifiable information and sensitive personally identifiable information in incident tickets and disconnect the current incident tracking system from the network by September 30, 2018.	12/31/19
	2. Update standard operating procedures for EPA incident tracking system help desk technicians. Establish controls for technicians to comply with federal personally identifiable information requirements when they handle incident tickets that require them to collect personally identifiable information and sensitive personally identifiable information.	EPA management indicated that standard operating procedures were updated on July 31, 2018, and provided a copy of the updated procedures.	7/31/18
	3. Complete a System of Records Notice for the replacement incident tracking system.	A new System of Records Notice for the replacement incident tracking system will be completed at the end of the third quarter in FY 2019.	6/30/19
	4. Update the EPA's system security plan, privacy impact assessment, and other necessary security documentation to specify that the replacement system will contain personally identifiable information and sensitive personally identifiable information.	System security plan, privacy impact assessment, and other necessary documentation for ServiceNow and Remedy will be updated to reflect what is in the recommendation.	12/31/20

19-P-0158, Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats, May 21, 2019	We recommend that the **assistant administrator for Mission Support**: 2. Establish a process to periodically review the Agency's information security weakness tracking system's settings to validate that each setting is appropriately implemented and compliant with the Agency's standards.	The EPA concurs with the recommendation and will establish a process to periodically review settings in the Agency's information security weakness tracking system to validate that each setting is appropriately implemented and compliant with the Agency's standards	10/31/20
	3. Collaborate with the vendor of the Agency's information security weakness tracking system to determine whether audit logging to capture "all data changes" is an available security feature within the Agency's information security weakness tracking system and, if so, activate the audit log settings to capture all data changes. If audit logging is not available, establish compensating controls within the Agency's information security weakness tracking system that would record or describe what data has been changed.	The EPA concurs with the first part of the recommendation and will continue to collaborate with the vendor to determine whether audit logging to capture "all data changes" is an available security feature within the Agency's information security weakness tracking system and, if so, activate the audit log settings to capture all data changes.	10/31/20
		The EPA partially concurs with the second part of the recommendation. Given that the audit log function built into an application is the control within that application to record changes, it is unlikely compensating controls will be available within the tool. However, the EPA will review possibilities and implement what can be reasonably accomplished within the tool.	11/30/20
19-P-0195, Pesticide Registration Fee, Vulnerability Mitigation and Database Security Controls for EPA's FIFRA and PRIA Systems Need Improvement, June 21, 2019	We recommend that the **assistant administrator for Chemical Safety and Pollution Prevention**: 2. Complete the actions and milestones identified in the Office of Pesticide Programs' Pesticide Registration Improvement Act Maintenance Fee Risk Assessment document and associated plan regarding the fee payment and refund posting processes.	The Office of Pesticide Programs will research the feasibility of utilizing an automated solution for posting fee payments and fee refunds. As a first step, the OPP will investigate the possibility of utilizing the Pesticide Submission Portal to allow the registrants to submit fee payments. By October 2019, a document of findings will be presented to the OPP senior leadership team for consideration.	12/31/20
	4. Implement controls to comply with federally required time frames to install patches to correct identified vulnerabilities in the Pesticide Registration Information System.	Currently, the OMS manages the automated patch management systems called Continuous Diagnostics Monitoring and Big Fix to determine patches and the state of information system components with regards to flaw remediation, such as software patching, in accordance with the National Institute of Standards and Technology Special Publication 800-53r4 SI-2(1), SI-2(2). The OPP will comply with OMS guidance for federally required time frames to install patches to correct identified vulnerabilities in Pesticide Registration Information System and the Office of Pesticide	10/31/19
	5. Implement the EPA's patch management process for the Pesticide Registration Information System.		

		Programs local area network. By October 2019, OPP will update its PRISM and OPP LAN System Security Plan to reflect these procedures.	
20-P-0007, Management Alert: EPA Still Unable to Validate that Contractors Received Role-Based Training for Information Security Protection, October 21, 2019	We recommend that the **assistant administrator for Mission Support:** 3. Implement a plan to analyze the EPA's information technology services contractual agreements initiated prior to EPA Acquisition Guide 39.1.2 to (a) determine how many of these agreements require modification to include role-based training requirements and (b) include the training requirements in the respective agreements	The OMS will issue a memorandum to senior resource officials, junior resource officials, Office of Acquisition Solutions division directors, and Regional Acquisition managers by January 28, 2020, requiring contracting officers in concert with program contracting officer's representatives and OMS Environmental Information representatives, to review and analyze active information technology services contractual agreements, and ascertain that role-based training requirement is included when contractual agreements require EPA contractors to perform work that has significant information security responsibilities. Where language is discovered to be absent, contracting officers will modify the contracts to include role-based training requirement language. The OMS will request that SROs certify completion of the review, analysis, and inclusion of role-based training requirement language in IT contracts under their cognizance.	4/10/20
20-E-0309, EPA Needs to Improve Processes for Securing Region 8's Local Area Network, September 10, 2020	We recommend that the **chief financial officer:** 6. Coordinate with regions to implement internal controls to determine whether personally identifiable information is protected on regional Superfund Cost Recovery Package Imaging and Online System servers.	The Office of the Chief Financial Officer's Office of Technology Solutions will coordinate with EPA regions to implement a Memorandum of Understanding. The intent is for the MOU to require each regional senior information official to certify that PII on regional SCORPIOS servers is protected in accordance with EPA's Information Technology Security policies. Estimated timing to complete the documents is October 30, 2020. In addition to the MOU with each of the EPA regions, the OCFO has identified nearly 20,000 PII records that may be appropriate to remove from the regional databases. The OCFO will work with regional contacts to verify and delete the records which will further reduce risk of PII disclosure.	10/30/20

*The position titles have changed since the respective reports were issued.