



U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

*Compliance with the law
Operating efficiently and effectively*

Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats

Report No. 19-P-0158

May 21, 2019



Report Contributors:

Rudolph M. Brevard
Vincent Campbell
Eric Jackson Jr.
Tessa Waters

Abbreviations

CIO Chief Information Officer
EPA U.S. Environmental Protection Agency
OIG Office of Inspector General
POA&M Plan of Action and Milestones

Cover Image: Improper information security practices can lead to the exploitation of an information security system. (EPA OIG image)

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

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our [OIG Hotline](#).

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our [Email Updates](#)
Follow us on Twitter [@EPAoig](#)
Send us your [Project Suggestions](#)



At a Glance

Why We Did This Project

The Office of Inspector General (OIG) conducted an audit to determine whether the U.S. Environmental Protection Agency (EPA) completed and documented actions taken to remediate weaknesses in the agency's information security program.

Agency information security policy and procedures require personnel to create plans of action and milestones (POA&Ms) in the agency's information security weakness tracking system for those weaknesses that cannot be remediated within a specified timeframe. POA&Ms are an essential information security component in the agency's ability to combat cyber-security threats and strengthen its network and systems.

This report addresses the following:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

Address inquiries to our public affairs office at (202) 566-2391 or [OIG WEBCOMMENTS@epa.gov](mailto:OIG_WEBCOMMENTS@epa.gov).

List of [OIG reports](#).

Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats

What We Found

EPA personnel did not manage POA&Ms for remediating security weaknesses within the agency's information security weakness tracking system as required by EPA policy. This happened because the office responsible for identifying vulnerabilities relies on other agency offices to enter the POA&Ms in the tracking system to manage unremediated vulnerabilities. We identified one EPA office that was tracking vulnerabilities outside the tracking system, while another office indicated that it did not have a formal process to create POA&Ms in the system. Without accessible and consistent information about unremediated weaknesses, senior EPA managers cannot make risk-based decisions on how to protect the agency's network against cyber-security threats.

Missing POA&M data and incorrect security settings limit the EPA's ability to manage enterprise risk and strengthen its security posture.

Additionally, the EPA's information security weakness tracking system lacked controls to prevent unauthorized changes to key data fields and to record these changes in the system's audit logs. This occurred because the EPA neither enabled the feature within the tracking system to prevent unauthorized modifications to key data nor configured the system's logging feature to capture information on the modification of key data fields. As a result, unauthorized changes to the system's data could occur and hamper the agency's ability to remediate existing system weaknesses.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Mission Support establish a control to validate that agency personnel create required POA&Ms for vulnerability testing results. We also recommend that the Assistant Administrator establish a process to periodically review the agency's tracking system's security settings to validate that each setting meets the agency's standards, and collaborate with the tracking system's vendor to determine whether audit logging can capture all data changes.

The agency concurred with our recommendations and provided planned corrective actions with estimated completion dates. All recommendations are considered resolved with planned corrective actions pending.



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

OFFICE OF
INSPECTOR GENERAL

May 21, 2019

MEMORANDUM

SUBJECT: Insufficient Practices for Managing Known Security Weaknesses and System Settings Weaken EPA's Ability to Combat Cyber Threats
Report No. 19-P-0158

FROM: Charles J. Sheehan, Deputy Inspector General

A handwritten signature in blue ink that reads "Charles J. Sheehan".

TO: Donna J. Vizian, Principal Deputy Assistant Administrator
Office of Mission Support

This is our final report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY17-0139. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Information Security and Privacy within the Office of Mission Support is responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your office provided acceptable corrective actions and milestone dates in response to OIG recommendations. All recommendations are resolved and no final response to this report is required. However, if you submit a response, 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.

The report will be available at www.epa.gov/oig.

Table of Contents

Chapters

1	Introduction	1
	Purpose	1
	Background.....	1
	Responsible Offices	2
	Scope and Methodology	2
	Prior Audit Work.....	3
2	Personnel Did Not Develop Required POA&Ms for Security Weaknesses	5
	Lack of POA&Ms Weakens EPA’s Efforts to Strengthen Its Security Posture	5
	Conclusion	7
	Recommendation.....	8
	Agency Response and OIG Evaluation	8
3	Improved Security Settings Needed for EPA’s Information Security Weakness Tracking System	9
	Unlocked Data Field in Tracking System Could Lead to Unauthorized Changes	9
	Audit Logs Do Not Capture Data Changes Within Tracking System.....	10
	Conclusion	11
	Recommendations	11
	Agency Response and OIG Evaluation	11
	Status of Recommendations and Potential Monetary Benefits	13

Appendices

A	OIG Reports Highlighting Weaknesses in EPA’s Vulnerability and POA&M Management Practices	14
B	Agency Response to Draft Report	16
C	Distribution	19

Chapter 1

Introduction

Purpose

The U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) announced an audit to determine whether the agency:

1. Completed required background investigations for contractor personnel with privileged accesses to EPA information systems.
2. Completed and documented actions taken to remediate weaknesses in the agency's information security program.

To address the first objective, the OIG issued *Management Alert: EPA Has Not Initiated Required Background Investigations for Information Systems Contractor Personnel*, Report No. [17-P-0409](#), dated September 27, 2017. We recommended that the agency implement controls over the EPA's personnel screening practices for initiating the required high-level background investigation for contractor personnel with privileged access to agency networks, information systems and data. The EPA's Management Audit Tracking System specifies that the agency completed the corrective actions for the recommendation. This current report only addresses the second objective.

Background

The EPA implemented an automated tool for managing the agency's plan of action and milestones (POA&M) process. This automated tool has the capability to maintain a catalog of known information security weaknesses. The tool also enables the agency to continuously manage and track remediation actions for identified information system weaknesses and serves as a critical component of the EPA's risk management program.

A POA&M is a corrective action plan that identifies tasks that need to be accomplished to remediate known weaknesses in an information system or program.

The Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, dated July 15, 2016, states that management retains overall responsibility and accountability for controls related to the processes provided a third party and must monitor the process as a whole to make sure it is effective.

The National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013, states that organizations may

implement compensating security controls when the organization is unable to effectively implement specific security controls.

The EPA’s Chief Information Officer (CIO) indicates in CIO 2150.4, *Information Security Policy*, dated December 28, 2016, that the EPA’s information security program will operate at all levels within the agency and include a process for planning, developing, implementing, evaluating and documenting remedial actions to address deficiencies in information security controls.

The EPA’s CIO 2150-P-04.2, *Information Security - Security Assessment and Authorization Procedures*, dated May 27, 2016, requires agency personnel to document information security weaknesses and planned remedial actions in the agency’s information security weakness tracking system. These procedures identify individuals responsible for managing POA&Ms. Table 1 lists the key personnel roles and responsibilities for managing POA&Ms in the agency’s information security weakness tracking system.

Table 1: Key roles and responsibilities for managing POA&Ms

Roles	Responsibilities
Senior Information Officer	Provide input and assist with acquiring funding and resources for POA&Ms.
System Owner	Develop, manage and update POA&Ms.
Information Security Officer	Manage POA&Ms.
Information System Security Officer	Enter POA&Ms and maintain current and accurate information.

Source: EPA CIO 2150-P-04.2.

Responsible Offices

The Office of Mission Support provides technology services and manages the EPA’s information technology investment. Within the Office of Mission Support, the Office of Information Security and Privacy is responsible for:

- Ensuring the agency is compliant with federal and EPA information security directives.
- Managing the agency’s information security system operations.
- Conducting continuous monitoring assessments of EPA systems.
- Conducting reviews of POA&M data for accuracy and completeness.

Each EPA program and regional office has information security personnel designated as points of contact to manage POA&Ms in accordance with agency information security requirements.

Scope and Methodology

We performed this audit from March 2017 through January 2019 in accordance with generally accepted government auditing standards. Those standards require

that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We reviewed publications issued by the National Institute of Standards and Technology, and agency policies and procedures for establishing and managing POA&Ms. We interviewed agency personnel and contractors on their oversight roles for data quality of POA&M information for remediation of known information security weaknesses. We conducted a walk-through of the system configuration settings to determine whether settings were established and in accordance with agency policy and procedures, and federal security publications.

The Office of Information Security and Privacy provided us a listing of POA&Ms extracted from the agency's information security weakness tracking system. We judgmentally selected a sample of these POA&Ms to determine the status of corrective actions to remediate the known weaknesses by the scheduled completion date. We evaluated the EPA's efforts for documenting and completing POA&Ms to remediate weaknesses through inquiries, observation and review of documentation.

Prior Audit Work

The OIG has issued several reports indicating that the EPA needs to make improvements in its vulnerability management and POA&M processes. Those reports included the following:

- On November 16, 2015, we issued Report No. [16-P-0039](#), *Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of EPA's Information Security Program*. We reported that the EPA needs improvement in its processes to ensure that resources and costs needed to remediate vulnerabilities are identified on the agency's network and connected devices. We did not issue any recommendations, but briefed EPA personnel on our analyses and the agency agreed with our results.
- On October 14, 2015, we issued Report No. [16-P-0006](#), *EPA Needs to Improve Security Planning and Remediation of Identified Weaknesses in Systems Used to Protect Human Health and the Environment*. We reported that while the EPA indicated it took steps to improve the completeness and accuracy of reported information system security data, EPA security personnel were not developing a required POA&M in a timely manner to manage the remediation of known vulnerabilities as required by agency policy and procedure. The EPA took actions on four of the five recommendations prior to the issuance of the final report. We followed up on the unimplemented recommendation, which required the EPA to develop and implement a process using the agency's information security weakness tracking system to manage vulnerabilities, especially high-risk

vulnerabilities. Based on our audit work performed, we determined that the EPA completed the remaining recommendation.

See Appendix A for a full listing of previous EPA OIG information security reports identifying deficiencies in the EPA's vulnerability management and POA&M processes.

Chapter 2

Personnel Did Not Develop Required POA&Ms for Security Weaknesses

EPA information security policy and procedures require agency and contractor personnel to create POA&Ms in the agency's tracking system whenever remediation cannot be completed within the EPA's required timeframes. However, EPA personnel did not manage unremediated weaknesses within the agency's information security tracking system as required by agency policy and procedures. This occurred because the agency did not automatically record the identified weaknesses into its information security weakness tracking system when the EPA conducted monthly vulnerability testing of its network. As a result, the unremediated weaknesses in the agency's network and information systems could be exploited to weaken the agency's ability to combat cyber security threats.

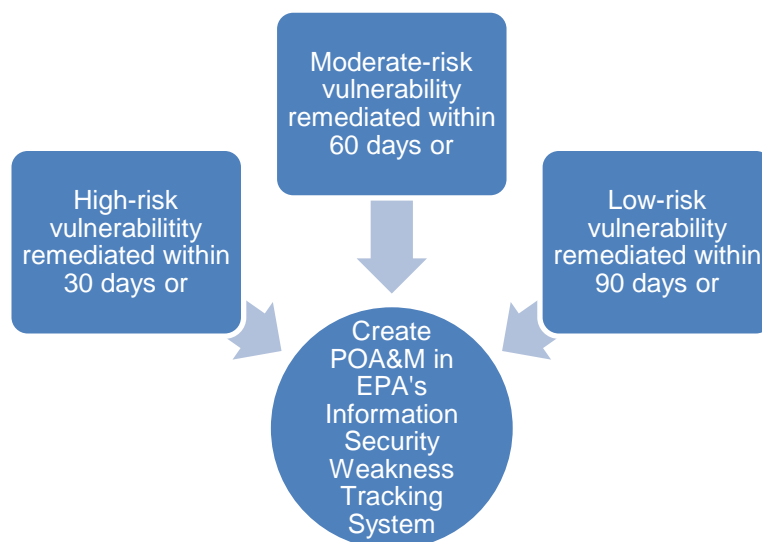
Lack of POA&Ms Weakens EPA's Efforts to Strengthen Its Security Posture

EPA personnel did not create the required POA&Ms to correct unremediated weaknesses for their respective systems. The EPA's CIO 2150-P-04.2, *Information Security - Security Assessment and Authorization Procedures*, dated May 27, 2016, requires information security personnel to document and manage POA&Ms for the discovered vulnerability within the agency's tracking system. The procedures further explain that POA&Ms shall be developed from any source, including, but not limited to, the following:

- (1) Reviews, tests, audits or assessments;
- (2) Security impact assessment;
- (3) Independent verification and validation findings;
- (4) Continuous monitoring activities;
- (5) Incidents; and
- (6) Routine maintenance and administration.

Figure 1 identifies the maximum number of days the EPA procedure allows for personnel to mitigate or remediate weaknesses based on the level of risk (high, moderate or low) before personnel must create a POA&M within the agency's information security weakness tracking system.

Figure 1: Timeframes to remediate weaknesses by level of risk



Source: EPA CIO 2150-P-04.2.

The EPA's vulnerability management program conducts monthly testing of devices connected to the EPA's network to identify weaknesses that require remediation and reporting. The agency states that the purpose of the program is to deploy a continuous network monitoring program to reduce the agency's vulnerability to cyber-security attacks as a means of securing critical computer networks. Vulnerability management personnel distribute monthly vulnerability reports to EPA offices that identify devices with weaknesses and categorize the level of risk (high, moderate or low) associated with each weakness.

The EPA's POA&M Guide states that the information system security officer and system owners are to develop and implement corrective action plans for weaknesses identified in their systems. The POA&Ms are not immediately created once the vulnerability testing is completed, which results in EPA offices not always creating POA&Ms for weaknesses that were not remediated within the agency's prescribed timeframes. For example:

- One information security person indicated that their office does not enter the results of vulnerability scans and other weaknesses identified into the agency's information security weakness tracking system, but rather they are tracking and managing the reported weaknesses on a spreadsheet. The person indicated their office took this action to prevent external parties within the EPA from having oversight of their office's remediation activities.
- One headquarters program office had not created POA&Ms in the agency's information security weakness tracking system for 10 high-risk vulnerabilities identified on their servers. It was discovered that the 10 high-risk vulnerabilities remained unremediated for more than the 30 days allowed by the policy. Agency personnel indicated their headquarters

program office did not have a formal process for creating POA&Ms within the agency's information security weakness tracking system to remediate the vulnerabilities identified by the EPA's network scans.

Failing to create POA&Ms for known vulnerabilities is a recurring issue within the EPA, as demonstrated by the several OIG reports issued over the past 10 years (see Appendix A) indicating that the EPA needs to improve its vulnerability management and POA&M processes. Remediation of security weaknesses with POA&Ms is essential to achieving a mature and effective information security program. The EPA's not immediately creating POA&Ms for weaknesses when they are identified leads to management not having the information necessary to make risk-based decisions; and impedes the EPA's information security strategy to assure the confidentiality, integrity and availability of users' information and agency resources.

We met with EPA management subsequent to our issuing a discussion document outlining our findings and recommendations. EPA management indicated:

- The POA&M monitoring and validation process serves as the EPA's oversight process for POA&M activities. The EPA is designing an operational process to interface vulnerability testing conducted by the Office of Information Security and Privacy with the POA&M monitoring and validation, and patch management processes.
- The vulnerability management team transitioned from the security operation center to the Office of Information Security and Privacy, and the POA&M monitoring and validation process has been in place since 2013.
- Due to limited resources, the EPA cannot track 100 percent of the vulnerability testing results and personnel are limited to reviewing a sample each year. The EPA is implementing a continuous diagnostics and mitigation program with dashboard capabilities that will provide more real-time visibility on the security health of the agency's network and systems. EPA management provided documentation that indicates the continuous diagnostic and mitigation program commenced in fiscal year 2017 and will be incorporated through multiple phases over several years, with expected final implementation in fiscal year 2019.

We believe vulnerability management and remediation is a shared responsibility amongst all EPA offices. However, our information security audits continue to find that agency personnel are not entering POA&Ms into the tracking system when they are required to do so.

Conclusion

As indicated in Appendix A, the OIG has consistently identified managing information security weaknesses with POA&Ms as a deficiency within the EPA's

information security program. POA&Ms play an essential information security role in the agency's ability to combat threats and strengthen the agency's network and systems by:

- Providing descriptive information on the vulnerability/weakness.
- Defining priorities for resolving the vulnerability/weakness.
- Supporting the justification for and allocation of resources.
- Providing status of remediation efforts.

Without documenting this essential information as required, the EPA's network and systems are at risk of exploitation by cyber techniques that will weaken the agency's ability to combat against denial of service events, unauthorized access, and destruction of sensitive data and leakage of propriety information to external sources.

Recommendation

We recommend that the Assistant Administrator for Mission Support:

1. Establish a control to validate that agency personnel are creating the required plans of action and milestones for those weaknesses identified from the vulnerability testing but not remediated within the agency's established timeframes per the EPA's information security procedures.

Agency Response and OIG Evaluation

The Office of Mission Support concurred with Recommendation 1 and provided planned corrective actions. The EPA indicated that it will continue to mature the new vulnerability management process as the agency transitions from monthly to 72-hour scan cycles. The EPA stated that it will analyze the risks associated with the vulnerabilities and then develop and implement a strategy to manage the risk. The agency's initial planned corrective actions for the development and implementation of the strategy did not include a milestone. The EPA subsequently provided an updated corrective action plan with a milestone date for implementing the strategy. As part of the strategy, the EPA further acknowledged that it would implement an appropriate control to validate that agency personnel are creating POA&Ms to manage weaknesses from vulnerability scans. Based on the additional information provided by the Office of Mission Support, we revised Recommendation 1 accordingly and believe the proposed corrective actions will satisfy the intent of the revised recommendation. Recommendation 1 is considered resolved with corrective actions pending.

Appendix B contains the full written response from the EPA.

Chapter 3

Improved Security Settings Needed for EPA's Information Security Weakness Tracking System

The EPA lacked two key management controls over its information security weakness tracking system: controls that allow only authorized activities to occur and controls that reflect data modification in audit logs. The U.S. Government Accountability Office's *Standards for Internal Controls in the Federal Government* requires security management to design controls to protect an entity from inappropriate access and unauthorized use of a system. The EPA did not set up the information security weakness tracking system to prevent modifications. In addition, the EPA contractor did not configure the system's logging feature to capture information when personnel modify data inside key data fields. As a result, unauthorized changes to system data or controls limit the agency's ability to prevent the exploitation of existing weaknesses and detect cyber attacks within EPA systems.

Unlocked Data Field in Tracking System Could Lead to Unauthorized Changes

The EPA's security settings did not prevent users from making modifications to POA&M data. Specifically, the security setting for the scheduled completion date field was set to "unlock." The EPA uses the "scheduled completion date" to age POA&Ms and identify those vulnerabilities and weaknesses 30, 60 and 90 days overdue for resolution.

Scheduled completion data is based on a realistic timeframe for what it will take to allocate the required resources and test and implement corrective actions to remediate information security weaknesses.

The U.S. Government Accountability Office's *Standards for Internal Controls in the Federal Government* (GAO-14-704G), dated September 2014, requires security management to design control activities over access to protect an entity from inappropriate access and unauthorized use of the system. Additionally, Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, dated July 15, 2016, states that management retains overall responsibility and accountability for controls related to the processes provided by the third party, and must monitor the process as a whole to make sure it is effective.

EPA contractors responsible for managing the agency's information security weakness tracking system indicated that the scheduled completion date field was not reset after making a system modification. We learned that periodic reviews of security settings were not performed to verify whether the settings were "locked." EPA personnel indicated that there is no requirement for the contractors to

periodically review the system's security settings. With an "unlock" security setting, users can arbitrarily make numerous changes to the "scheduled completion date" for each POA&M, which would hamper the EPA's ability to determine if timely remedial actions are implemented to reduce exploitation from cyber-security attacks.

Audit Logs Do Not Capture Data Changes Within Tracking System

The audit logs within the agency's information security weakness tracking system do not capture or track data changes that occurred in the system. Agency contractor personnel indicated that the existing audit log was not configured to capture all system changes. For example, the contractors reset the security setting for the scheduled completion date field from "unlock" to "lock." The audit log captured only the user's name and that a modification was made to that data field. The audit log did not specifically identify the action the user initiated (e.g., changed security setting from "unlock" to "lock") to the scheduled completion date field. EPA personnel did not know whether the system's audit logging feature had the capability to log "all changes made" to data fields. Collecting this descriptive information would provide the EPA with evidence to hold a user accountable for any authorized or unauthorized changes to the information system.

Effective log management is essential to both security and compliance. Audit logging provides the EPA with the transparency it will need to understand system changes that are made within the agency's information security weakness tracking system. Audit logs of what data has changed will not only provide a detailed roadmap of those changes that are authorized but, importantly, also identify unauthorized internal and external access and cyber-security breaches.

The EPA's CIO 2150-P-03.2, *Information Security - Audit and Accountability Procedures*, dated September 28, 2015, requires identification within audit logs of modifications to applications, system administration activities, and privileges and access controls. However, the security plan for the agency's information security weakness tracking system did not document that the EPA developed and implemented compensating controls to capture the detailed events of the modifications and system administration activities that occur within the system.

The National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, dated April 2013, indicates that organizations may find it necessary to implement compensating security controls when the organization is unable to effectively implement specific security controls within the system's environment. The publication states that compensating controls are alternative security controls that provide equivalent or comparable protection for information systems and the information processed, stored or transmitted by the systems.

In the EPA's response to our discussion document, EPA management indicated that the agency had resolved the issue we identified with the scheduled completion date field by setting it to "lock." The EPA submitted documentation to demonstrate that the security setting has been set to "lock." However, it is incumbent upon the agency to periodically review the information security weakness tracking system's setting to verify that the system remains compliant with management's intent.

EPA management indicated that they have consulted with the vendor of the agency's information security weakness tracking system to request audit logging that will capture data changes. EPA management indicated those conversations are ongoing and they have not yet reached a decision on the solution.

Conclusion

Application security controls play a vital role in protecting data from authorized access, use and destruction. By properly setting controls and meeting prudent information security practices, the EPA will strengthen its security posture to minimize its exposure to cyber-security attacks.

Recommendations

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.
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.

Agency Response and OIG Evaluation

The Office of Mission Support concurred with Recommendation 2 and provided planned corrective actions. The EPA stated that it 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. We believe that the proposed corrective actions will satisfy the intent of the recommendation, and Recommendation 2 is considered resolved with corrective actions pending.

Initially, the Office of Mission Support partially concurred with Recommendation 3 and provided planned corrective actions. The EPA stated that it will collaborate with the vendor and, if available, activate the settings to capture the data changes. The EPA partially concurred with the second part of the recommendation. The EPA stated that audit logs are the controls to record changes and that it's unlikely compensating controls are available within the system. However, the EPA indicated that it will review and implement other possibilities that can be reasonably accomplished within the system. In a subsequent follow-up on the EPA's planned actions, the EPA indicated that modifying the existing audit logging function would result in expensive development costs.

As an alternative, the EPA indicated that it has commenced a research project to identify and procure a system that will include extensive audit logging capabilities. We believe that the proposed corrective actions will satisfy the intent of the recommendation, and Recommendation 3 is considered resolved with corrective actions pending.

Appendix B contains the full written response from the EPA.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status ¹	Action Official	Planned Completion Date	Potential Monetary Benefits (in \$000s)
1	8	Establish a control to validate that agency personnel are creating the required plans of action and milestones for those weaknesses identified from the vulnerability testing but not remediated within the agency's established timeframes per the EPA's information security procedures.	R	Assistant Administrator for Mission Support	12/31/21	
2	11	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.	R	Assistant Administrator for Mission Support	10/31/19	
3	11	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.	R	Assistant Administrator for Mission Support	11/30/19	

¹ C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

OIG Reports Highlighting Weaknesses in EPA's Vulnerability and POA&M Management Practices

The EPA OIG issued information security reports identifying deficiencies within the EPA's vulnerability management and POA&M processes. Table 2 list some of the OIG reports along with the reported weaknesses.

Table 2: Previously reported vulnerability management and POA&M weaknesses

OIG report title, number and date	Reported weaknesses
Fiscal Year 2015 Federal Information Security Modernization Act Report: Status of EPA's Information Security Program Report No. 16-P-0039 , November 16, 2015	The EPA needs improvement in its processes to ensure that resources and costs needed to remediate vulnerabilities are identified on the agency's network and connected devices.
EPA Needs to Improve Security Planning and Remediation of Identified Weaknesses in Systems Used to Protect Human Health and the Environment Report No. 16-P-0006 , October 14, 2015	EPA security personnel are not developing a required POA&M in a timely manner to manage the remediation of known vulnerabilities as required by agency policy and procedure. As a result, the EPA cannot be assured that the agency's tracking system provides the protection necessary to safeguard key information security data needed for decision-making and external reporting. Furthermore, known vulnerabilities continue to place the EPA's network at risk to be exploited because management lacks information to implement remediation activities.
Fiscal Year 2014 Federal Information Security Management Act Report: Status of EPA's Computer Security Program Report No. 15-P-0020 , November 13, 2014	The EPA did not ensure POA&Ms provided resources and ownership for correcting weaknesses nor did it ensure that costs associated with remediating weaknesses were identified.
Fiscal Year 2013 Federal Information Security Management Act Report: Status of EPA's Computer Security Program Report No. 14-P-0033 , November 26, 2013	The agency should take steps to improve processes for timely remediation of scan result deviations.
Results of Technical Network Vulnerability Assessment: EPA's Region 6 Report No. 12-P-0659 , August 10, 2012	Our vulnerability testing of networked resources located at Region 6 facilities identified Internet Protocol addresses with potentially 35 critical-risk, 217 high-risk, and 878 medium-risk vulnerabilities. If not resolved, these vulnerabilities could expose EPA assets to unauthorized access and potentially harm the agency's network.
Results of Technical Vulnerability Assessment: EPA's Directory Service System Authentication and Authorization Servers Report No. 11-P-0597 , September 9, 2011	Vulnerability testing of the EPA's directory service system authentication and authorization servers conducted in March 2011 identified authentication and authorization servers with numerous high-risk and medium-risk vulnerabilities. If not resolved, these vulnerabilities could expose EPA assets to unauthorized access and potentially harm the agency's network.

OIG report title, number and date	Reported weaknesses
Results of Technical Network Vulnerability Assessment: EPA's Ronald Reagan Building Report No. 10-P-0212 , September 7, 2010	Vulnerability testing of the EPA's Ronald Reagan Building network conducted in June 2010 identified Internet Protocol addresses with numerous high-risk and medium-risk vulnerabilities. If not resolved, these vulnerabilities could expose EPA assets to unauthorized access and potentially harm the agency's network.
Results of Technical Network Vulnerability Assessment: EPA's Potomac Yard Buildings Report No 09-P-0188 , June 30, 2009	Vulnerability testing of the EPA's Potomac Yard buildings network conducted during April 2009 indicated several high-risk vulnerabilities. If not resolved, these vulnerabilities could expose EPA assets to unauthorized access and potential harm to the agency's network.

Source: EPA OIG reports.

Agency Response to Draft Report



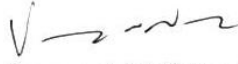
UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF MISSION SUPPORT

APR 15 2019

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report No. OA-FY17-0139
"Insufficient Practices for Managing Known Security Weaknesses and System
Configuration Settings Weaken EPA's Ability to Combat Cyber Threats" dated
January 31, 2019

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

TO: Rudolph Brevard, Director
Information Resources Management Directorate

Thank you for the opportunity to respond to the issues and recommendations in the subject audit report. Following is a summary of the agency's overall position, along with its position on each of the report recommendations. For those report recommendations with which the agency agrees, we have provided either high-level intended corrective actions and estimated completion dates to the extent we can or reasons why we are unable to provide high-level intended corrective actions and estimated completion date at this time.

AGENCY'S OVERALL POSITION

The EPA agrees with the Office of Inspector General's (OIG) overall report, that identifying and mitigating known weaknesses is an important aspect of ensuring the security of the agency's information assets. The EPA further agrees with the OIG's report in that the EPA has been improving capabilities in this area over the past several years but there is room for improvement.

Agreements

No	Recommendation	High-Level Intended Corrective Action(s)	Estimated Completion by Quarter and FY
1	<p>We recommend that the Assistance Administrator for Mission Support:</p> <p>Establish a control to validate that agency personnel are creating the required plans of action and milestones for those weaknesses identified from the vulnerability testing but not remediated within the agency’s established timeframes per the EPA’s information security directives.</p>	<p>The EPA will continue to mature the new vulnerability management process as the agency transitions from monthly to 72-hour scan cycles. The EPA will analyze the risks associated with vulnerabilities given impact, resources and increased visibility resultant from improved continuous monitoring capabilities to determine an appropriate scope of validation. The EPA will develop and implement a strategy based on the analysis results.</p>	<p>Analysis - by Q1 FY21 October 29</p> <p>Strategy Development and Implementation - by Q1 FY22</p>
2	<p>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.</p>	<p>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.</p>	<p>By Q1 FY20 October 31</p>
3	<p>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</p>	<p>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.</p> <p>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</p>	<p>1st Part - by Q1 FY20 October 31</p> <p>2nd Part Review - by Q1 FY20 November 30</p>

	information security weakness tracking system that would record or describe what data has been changed.	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.	
--	---	---	--

Disagreements

None.

CONTACT INFORMATION

If you have any questions regarding this response, please contact Lee Kelly, Division Director of the Office of Information Security and Privacy’s Training Compliance and Oversight Division on (202) 566-1197 or Marlyn Aguilar, Program Analyst, on (202) 566-0012.

Distribution

The Administrator
Associate Deputy Administrator and Chief of Operations
Chief of Staff
Deputy Chief of Staff
Assistant Administrator for Mission Support
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer,
Office of Mission Support
Director, Information Security and Management Staff, Office of Mission Support
Senior Information Officer, Office of Mission Support
Director, Office of Continuous Improvement, Office of the Administrator
Director and Chief Information Security Officer, Office of Information Security and Privacy,
Office of Mission Support
Director, Office of Information Technology Operations, Office of Mission Support
Director, Office of Resources and Business Operations, Office of Mission Support
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Mission Support