U.S. Environmental Protection Agency
Office of Inspector General

19-P-0158
May 21, 2019

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.

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

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

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.

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.