U.S. Environmental Protection Agency
Office of Inspector General

16-P-0259
August 10, 2016

At a Glance

Why We Did This Review

The Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA) conducted this audit to determine to what extent the EPA implemented information system security policies and procedures to protect agency systems that provide access to national security or Personally Identifiable Information (PII), as outlined in Section 406 of the Cybersecurity Act of 2015.

This report addresses the following EPA goal or cross-agency strategy:

- *Embracing EPA as a high-performing organization.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

Cybersecurity Act of 2015 Report: EPA's Policies and Procedures to Protect Systems With Personally Identifiable Information

What We Found

Section 406 of the Cybersecurity Act of 2015 calls for Inspectors General of agencies with covered systems to report on several aspects of the covered systems' information system security controls. The term "covered system" means a national security system as defined in 40 U.S.C. § 11103 or a federal computer system that provides access to PII.

The EPA has 30 systems that contain sensitive PII. Safeguarding information and preventing system breaches are essential for ensuring the EPA retains the trust of the American public.

The EPA has 30 covered systems that contain sensitive PII covered by provisions of the act. Of the 30 covered systems, two were sampled for our audit. Although the EPA has 30 systems that include sensitive PII, the EPA does not own any systems that include national security information.

The act requires Inspectors General to report on the areas identified in the bullets below. We provided information in the following eight areas based on the requirements outlined in the act for the EPA's covered systems.

- Description of logical access policies and practices.
- Description of the logical access controls and multifactor authentication used to govern privileged users access.
- Reasons for not using logical access controls and multifactor authentication if applicable.
- Policies and procedures used to conduct inventories of software and licenses.
- Capabilities utilized to monitor and detect exfiltration and other threats.
- Description of how monitoring and detecting capabilities are utilized.
- Reasons why monitoring and detecting capabilities are not used if applicable.
- Description of policies and procedures used to ensure entities and contractors providing services to the EPA are implementing the information security management practices identified in the act.

We issued a draft report containing our conclusions and briefed EPA representatives on the audit results. The EPA agreed with our results and emailed its responses, which were evaluated and incorporated into this report.

The full version of this report contained controlled unclassified information. This is a redacted version of that report, which means the controlled unclassified information has been removed. The redactions are clearly identified in the report.