U.S. Environmental Protection Agency
Office of Inspector General

14-P-0033
November 26, 2013

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency's (EPA's) Office of Inspector General (OIG) conducted this review to assess the EPA's compliance with the Federal Information Security Management Act (FISMA). FISMA requires Inspectors General to prepare an annual evaluation of their agencies' information security programs and practices. The Department of Homeland Security issued reporting guidelines requesting information on 11 information system security practices within federal agencies.

This report addresses the following EPA theme:

- *Embracing EPA as a high performing organization.*

For further information, contact our public affairs office at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2014/20131126-14-P-0033.pdf

Fiscal Year 2013 Federal Information Security Management Act Report: Status of EPA's Computer Security Program

What We Found

The EPA has established an agencywide information security program that assesses the security state of information systems that is consistent with FISMA requirements and applicable policy and guidelines for the following areas:

- Continuous Monitoring Management
- Identity and Access Management
- Incident Response and Reporting
- Security Training
- Plan of Action and Milestones
- Remote Access Management
- Contingency Planning
- Security Capital Planning

The EPA's network and data could be exploited without processes to evaluate risks and timely remediate vulnerabilities. Data processed by EPA contractors could be at risk because adequate controls may not be in place.

However, the EPA should place more management emphasis on remediating significant deficiencies found within the agency's configuration management, risk management and contractor systems management practices. The agency should take steps to:

- Improve processes for timely remediation of scan result deviations.
- Address risks from an organizational, mission and business, and information system perspective.
- Obtain sufficient assurance that security controls for contractor systems are effectively implemented and comply with federal and organization guidelines.

We briefed the agency on the results of our audit work and, where appropriate, made adjustments to address its concerns.