



At a Glance

Why We Did This Review

The Office of the Inspector General conducted this review to assess the U.S. Environmental Protection Agency's (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 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.

The full report is at: www.epa.gov/oig/reports/2014/20141113-15-P-0020.pdf

Fiscal Year 2014 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 for assessing the security state of information systems that is consistent with FISMA requirements and applicable policy and guidelines for the following areas:

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

The lack of a fully developed Configuration Management program places the EPA's network at a greater risk of being compromised.

However, the EPA should place more emphasis on remediating deficiencies found within the agency's Configuration Management program. Specifically, the agency should take steps to:

- Address deviations identified by scans in a timely manner.
- Maintain documentation of baseline scans of servers and network appliances.
- Install patches in a secure and timely manner.

Additionally, in conducting the review of the Contingency Planning section of FISMA, we found that the EPA currently has an outdated Business Impact Analysis.