U.S. Environmental Protection Agency
Office of Inspector General

15-P-0290
September 21, 2015

At a Glance

Why We Did This Audit

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to determine to what extent the EPA relies on contractor systems for information processing and programmatic support, and whether the EPA has implemented management-control processes to mitigate information security risks posed by the systems.

The EPA *System Life Cycle Management (SLCM) Procedure* details the system development phases, activities and documents necessary to properly manage and control the agency's information technology (IT) investments.

The EPA uses IT systems operated and maintained by contractors to conduct information collection and analysis. We learned from EPA OIG investigators that data maintained by a third party and residing at the vendor's site were breached on multiple occasions.

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/2015/20150921-15-P-0290.pdf

Incomplete Contractor Systems Inventory and a Lack of Oversight Limit EPA's Ability to Facilitate IT Governance

What We Found

Agency officials were unaware of which systems or services are required by the SLCM Procedure to be included in the EPA's authoritative information system database known as the Registry of EPA Applications, Models and Databases (READ). The READ inventory is important because it provides the tracking mechanism to ensure IT investments receive the appropriate level of oversight.

By not having a complete inventory of contractor systems, and by not assessing the operating effectiveness of contractor control environments in which systems are placed, the EPA risks being unable to protect its resources and data from undue harm.

Officials were also unaware of which stage of the system life cycle to enter contractor systems into READ, and in cases where multiple offices manage separate components of the same contractor system, which program office is responsible for updating READ. As a result, READ did not contain information on 22 contractor systems that are owned or operated on behalf of the EPA and are located outside of the agency's network. The registry also lacked information on 81 internal EPA contractor-supported systems.

We also found that personnel with oversight responsibilities for contractor systems were not aware of the requirements outlined in EPA information security procedures. As a result, EPA contractors did not conduct the required annual security assessments, did not provide security assessment results to the agency for review, and did not establish the required incident response capability. Without the required security controls, data breaches costing from $1.4 million to over $12 million could have occurred if all files within these systems were compromised.

Recommendations and Planned Agency Corrective Actions

We recommend that the Chief Information Officer update the 2015 READ data call instructions to include language from the agency's SLCM procedure. We also recommend that the Assistant Administrator for Administration and Resources Management designate responsible individual(s) to be the Primary Information Resource Steward(s) for READ records for the systems that comprise the Human Resources Line of Business, throughout the systems' life cycle.

In addition, we recommend that the Chief Information Officer implement the previously approved EPA Information Security Task Force recommendations for implementing a role-based training program, and for managing the annual security assessments and vulnerability management program. The EPA agreed with our recommendations and provided a corrective action plan with dates for each recommendation.