U.S. Environmental Protection Agency
Office of Inspector General

17-P-0344
July 31, 2017

At a Glance

Why We Did This Review

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to determine what processes the EPA uses to verify that agency contractors with significant information system security responsibilities meet established specialized training duties.

Role-based training is continuous education that improves current knowledge, skills and abilities for particular job functions. Under the Chief Information Officer's Federal Information Security Modernization Act (FISMA) Metrics, agencies are responsible for identifying and reporting specialized security training, such as role-based training, for all personnel (including contractors) with significant information security responsibilities.

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.

EPA Lacks Processes to Validate Whether Contractors Receive Specialized Role-Based Training for Network and Data Protection

What We Found

The EPA is unaware of the number of agency contractors who have significant information security responsibilities and require role-based training. This is attributed to the following factors:

- EPA personnel overseeing contractors are not aware of contractor role-based training requirements.
- The agency has not included role-based training requirements in all awarded contracts.
- The EPA lacks a process to track and report contractors' role-based training.

The EPA is unaware whether information security contractors possess the skills and training needed to protect the agency's information, data and network from security breaches.

In addition, the EPA did not report contractor training status in its fiscal years 2015 and 2016 Chief Information Officer's Annual FISMA reports submitted to the Office of Management and Budget. FISMA guidance requires agencies to train and oversee personnel (including contractors) who have significant responsibilities for information security, and report on the effectiveness of the information security program.

Insufficient awareness, contract requirements, and oversight of role-based training increase the risk that EPA contractors may lack the knowledge or skills necessary to protect the agency from cyberattacks. The agency also has insufficient information to manage risks to its data and network.

Recommendations and Planned Agency Corrective Actions

We recommend that the Assistant Administrator for Administration and Resources Management update the EPA Acquisition Guide to include the newly developed cybersecurity contract clauses that agency personnel must include in all EPA contracts, and include the cybersecurity contract clauses in all existing and future information technology contracts. We also recommend that the Office of Environmental Information implement a process for agency personnel to maintain a listing of contractor personnel required to take role-based training and report this information in the Chief Information Officer's Annual FISMA reports. The agency concurred with our recommendations and provided planned corrective actions with estimated completion dates. One recommendation has been resolved with corrective action completed. All remaining recommendations are resolved with corrective actions pending.