U.S. Environmental Protection Agency
Office of Inspector General

At a Glance

EPA's Information Systems and Data Are at Risk Due to Insufficient Training of Personnel With Significant Information Security Responsibilities

What the IPA Auditor Found

The EPA lacks an information security role-based training program that defines specific training requirements for personnel with significant information security responsibilities. Implementation of the EPA's information security training program is hindered by inconsistent assignment of information security roles across the various EPA offices. The current training program does not consider specific needs of technical and managerial personnel responsibilities for implementing information security as required by the federal guidance. Management has not completed efforts to tailor the existing training programs to align it with the EPA's organizational structure. The EPA's decentralized structure creates differing levels of information security implementation and oversight of training requirements. As a result, training may be insufficient to assure management that personnel with significant information security duties have the skills and understanding necessary to identify, prevent or mitigate vulnerabilities affecting the EPA's information systems and infrastructure.

> The EPA places its information systems and data at risk due to an organizational structure that has not specified required duties and responsibilities to ensure personnel are trained on key information security roles.

The IPA is responsible for the content of the audit report. The OIG performed the procedures necessary to obtain reasonable assurance about the IPA's independence, qualifications, technical approach and audit results. Having done so, the OIG accepts the IPA's conclusions and recommendations.

Recommendations and Agency Corrective Actions

The IPA's report recommends that the Assistant Administrator for Environmental Information: (1) define key information security aspects and duties for each security role; (2) provide additional training options specific to the federal information security environment and EPA information security roles; (3) standardize the terminology and definition of responsibilities for key IT security roles; and (4) provide clearer delineation of which EPA organizations should be responsible for delivering specific elements of information security role-based training. EPA agreed with the recommendations and is taking corrective action.

Noteworthy Achievements

The EPA conducts an annual Security and Operations conference. The EPA also implemented an annual specialized training requirement for employees with significant information security responsibilities.