At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency (EPA) (1) implemented and maintained database hardware and software in accordance with EPA policy requirements; and (2) secured critical financial information by restricting access to high-level database functions, such as database administrator authorities.

Background

EPA's core financial application, the Integrated Financial Management System (IFMS), shares data with many financial management system databases. An inadequately designed and implemented security control could be more easily breached, which could compromise the integrity of the data IFMS uses for financial reporting and decisionmaking.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link: www.epa.gov/oig/reports/2007/ 20070329-2007-P-00017.pdf

EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance

What We Found

We discovered weaknesses in how EPA offices (1) monitor databases for known security vulnerabilities, (2) communicate the status of critical system patches, and (3) monitor the use of and access to database administrator accounts and privileges. These weaknesses exist because EPA had not implemented security processes to (1) actively monitor systems that share data with IFMS, (2) share and collect information on the implementation of critical system patches, and (3) effectively manage access controls. Without these processes, the integrity of critical data in key Office of the Chief Financial Officer (OCFO) systems could be undermined. As a result, OCFO cannot ensure that the integrity of the data it provides to senior Agency officials is adequately protected.

We also identified specific technical weaknesses in three of the financial databases that share data with IFMS.

What We Recommend

We recommend that OCFO, the Office of Environmental Information (OEI), and the Office of Research and Development address areas where EPA could improve. Specifically, we recommend that:

- OCFO update the Memorandum of Understanding process to include formal security standards that require the program/regional offices to actively monitor the security status of systems that share data with IFMS.

- OEI strengthen, formalize, and evaluate the effectiveness of the followup procedures for obtaining complete responses from program and regional offices regarding high-level critical system patch alerts, as well as share status reports on the implementation of critical system patches.

- The system owners for each reviewed application correct all identified system weaknesses, and develop a Plan of Action and Milestones in the Agency's security weakness tracking system for all noted deficiencies.

The Agency agreed with all of our recommendations.

Due to the sensitive nature of the report's technical findings, we removed Appendices A, C, and D from the public version of the report.