U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00008
January 29, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine if access to and modification of mainframe system software at the U.S. Environmental Protection Agency (EPA) National Computer Center in Research Triangle Park in Raleigh, North Carolina, is controlled in accordance with Agency and Federal guidance, as well as best practices.

Background

The EPA's Office of Inspector General contracted KPMG, LLP (KPMG) to conduct an audit of mainframe system software. Controls over system software access and modifications are designed to (1) limit and/or monitor access to system software resources to protect against unauthorized modification, loss, and disclosure; (2) reduce the risk of the introduction of unauthorized changes; and (3) limit and monitor access to powerful system software programs.

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/2007/20070129-2007-P-00008.pdf

EPA Could Improve Controls Over Mainframe System Software

What KPMG Found

KPMG identified several weaknesses in EPA's internal controls over its mainframe system software, including:

- Roles and responsibilities were not clearly assigned.
- Change controls were not performed in accordance with Agency policies.
- Policies, procedures, and guides could be strengthened.
- Security settings for sensitive datasets and programs were not effectively configured or implemented.

As a result of these weaknesses, EPA is exposed to greater risk since its mainframe system software could potentially be compromised.

What KPMG Recommends

KPMG recommends that the Office of Environmental Information:

- Improve management oversight and review of primary support contractor activity, and clearly assign roles and responsibilities to ensure personnel are held accountable.
- Ensure change control procedures are performed in accordance with existing Agency and Federal guidance.
- Strengthen existing policies, procedures, and guides to establish standards for implementing key security controls for mainframe system software.
- Appropriately configure and implement security settings for sensitive datasets and programs.

This report contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of the report's technical findings, the Office of Inspector General removed Appendices A and B from the public version of the report.