OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Information Security Series: Security Practices

Clean Air Markets Division Business System

Report No. 2006-P-00024

May 4, 2006

Report Contributors: Rudolph M. Brevard
Charles Dade
Neven Morcos
Jefferson Gilkeson
Scott Sammons

Abbreviations

ASSERT	Automated Security Self-Evaluation and Remediation Tracking
C&A	Certification and Accreditation
CAMDBS	Clean Air Markets Division Business System
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act
NCC	National Computer Center
OAR	Office of Air and Radiation
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestone
RTP	Research Triangle Park

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00024
May 4, 2006

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

As part of our annual audit of the Environmental Protection Agency's compliance with the Federal Information Security Management Act (FISMA), we reviewed the security practices for a sample of key Agency information systems, including the Office of Air and Radiation's (OAR's) Clean Air Markets Division Business System (CAMDBS).

Background

FISMA requires agencies to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional damage to the Agency's information assets. CAMDBS is the data system EPA uses to support the market-based emissions trading 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/2006/20060504-2006-P-00024.pdf

Information Security Series: Security Practices Clean Air Markets Division Business System

What We Found

The Office of Air and Radiation (OAR) had substantially complied with many of the information security controls tested. In this regard, OAR developed and tested a contingency plan for the Clean Air Markets Division Business System (CAMDBS) and personnel with significant security responsibility completed the Agency's recommended specialized security training courses. However, our audit identified areas where OAR should place greater emphasis to comply with Federal and Agency information security requirements. We found that CAMDBS, a major application, was operating without (1) an up-to-date risk assessment and (2) effective practices to ensure that all production servers were monitored for known security vulnerabilities. OAR could have discovered the identified weaknesses had the office reviewed its implemented practices for completing these requirements as well as those of the National Computer Center (NCC), the group charged with primary responsibility for monitoring the servers. As a result, CAMDBS officials lacked key security management tools that could be used to proactively identify potential security weaknesses.

What We Recommend

We recommend that the CAMDBS System Owner:

- Conduct a full formal risk assessment of CAMDBS in accordance with Federal and Agency requirements.
- Coordinate with the NCC to verify that it is regularly monitoring all CAMDBS production servers for known vulnerabilities at least monthly.
- Develop a Plan of Action and Milestone in the Agency's information security weakness tracking system for all noted deficiencies.

We recommend that the OAR Information Security Officer:

- Conduct a review of OAR's current information security oversight processes and implement identified process improvements.

OAR agreed with the findings in the draft report and indicated that the office has moved forward aggressively to implement the recommendations. OAR's complete response is in Appendix A.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

May 4, 2006

MEMORANDUM

SUBJECT: Information Security Series: Security Practices
Clean Air Markets Division Business System
Report No. 2006-P-00024

TO: William Wehrum
Assistant Administrator for Air and Radiation

This is our final audit report on the information security controls audit of the Office of Air and Radiation's Clean Air Markets Division Business System. This audit report contains findings that describe problems the Office of Inspector General (OIG) has identified and corrective actions the OIG recommends. This audit report represents the opinion of the OIG, and the findings in this audit report do not necessarily represent the final U.S. Environmental Protection Agency (EPA) position. EPA managers, in accordance with established EPA audit resolution procedures, will make final determinations on matters in this audit report.

Action Required

In accordance with EPA Manual 2750, you are required to provide a written response to this report within 90 calendar days of the date of this report. You should include a corrective action plan for agreed upon actions, including milestone dates. We have no objection to further release of this report to the public. For your convenience, this report will be available at http://www.epa.gov/oig.

If you or your staff has any questions regarding this report, please contact Rudolph M. Brevard, Director, Information Technology Audits, at (202) 566-0893, or Charles Dade, Assignment Manager, at (202) 566-2575.

Bill A. Roderick
Acting Inspector General

Table of Contents

Purpose of Audit

Our objective was to determine whether the Office of Air and Radiation's (OAR's) Clean Air Markets Division Business System (CAMDBS) complied with Federal and Agency information security requirements. CAMDBS is the data system EPA uses to support the market-based emissions trading programs.

Background

We conducted this audit pursuant to Title III of the E-Government Act of 2002, commonly referred to as the Federal Information Security Management Act (FISMA). FISMA requires the Agency to develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional damage to the Agency's information assets. EPA's Chief Information Officer is responsible for establishing and overseeing an Agency-wide program to ensure the security of its network infrastructure is consistent with these requirements. Program office heads are responsible for ensuring that the security of each major application within their organization is managed in accordance with all appropriate government-wide and EPA-specific information technology policies, procedures, and standards.

Program offices should create a Plan of Action and Milestone (POA&M) when it identifies a security control weakness. The POA&M, which documents the planned remediation process, is recorded in the Agency's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool. ASSERT is used to centrally track remediation of weaknesses associated with information systems and serves as the Agency's official record for POA&M activity.

FISMA requires the Inspector General, along with the EPA Administrator, to report annually to the Office of Management and Budget (OMB) on the status of EPA's information security program. The OIG provided the results of its review to OMB in Report No. 2006-S-00001, *Federal Information Security Management Act, Fiscal Year 2005 Status of EPA's Computer Security Program.*

During our annual FISMA review, we selected one major application each from five EPA program offices and reviewed the office's security practices surrounding these applications. Our overall review noted instances where EPA could improve its security practices and the OIG reported the results to EPA's Chief Information Officer in Report No. 2006-P-00002, *EPA Could Improve Its Information Security by Strengthening Verification and Validation Processes*.

This audit report is one in a series of reports being issued to the five program offices that had an application reviewed. This report addresses findings and recommendations related to security practice weaknesses identified in OAR. In particular, this report summarizes our results regarding how OAR implements Federal and EPA security policies and procedures. This report also includes our

evaluation of how OAR implemented, tested, and evaluated CAMDBS' information security controls to ensure continued compliance with selected information security requirements. The Scope and Methodology section contains the specific information security controls audited during this review.

Scope and Methodology

We conducted our field work from March 2005 to July 2005 at EPA Headquarters in Washington, DC; and the National Computer Center (NCC), Research Triangle Park (RTP), North Carolina. We interviewed Agency officials at both locations and contract employees at the NCC. We reviewed relevant Federal and Agency information security standards. We reviewed application security documentation to determine whether it complied with selected standards. We reviewed system configuration settings and conducted vulnerability testing of servers for known vulnerabilities. We reviewed training records for personnel with significant security responsibilities.

We reviewed the following security practices for CAMDBS:

- **Security Certification and Accreditation (C&A) Practices** -- We evaluated whether application security plans, risk assessments, and authorizations for operation complied with Federal and Agency standards. We also reviewed the C&A package to determine whether the security plan was updated and re-approved at least every 3 years and the application was reauthorized at least every 3 years, as required by OMB (Office of Management and Budget) Circular A-130 and EPA policy.

- **Application Contingency Plans** -- We reviewed whether the contingency planning practices complied with requirements outlined in EPA Directive 2195A1 *(EPA Information Security Manual*), National Institute of Standards and Technology Special Publication 800-34 *(Contingency Planning Guide for Information Technology Systems*), and EPA Procedures Document *(Procedures for Implementing Federal Information Technology Security Guidance and Best Practices*).

- **Security Controls** -- We reviewed two areas of security controls: (1) system vulnerability monitoring, which included conducting vulnerability testing; and (2) physical controls. The NCC manages the servers that run CAMDBS and provides the primary security controls for the application. Therefore, when evaluating system vulnerability monitoring, we reviewed practices at the NCC. We did not test physical controls at the NCC, because the NCC was undergoing an audit of these controls at the time of our review and the audit found instances where EPA could improve its physical controls at RTP. The OIG reported the results of this audit in Report No. 2006-P-00005, *EPA Could Improve*

Physical Access and Service Continuity/Contingency Controls for Financial and Mixed-Financial Systems Located at its Research Triangle Park Campus.

- **Annual Training Requirements --** We reviewed whether employees with significant security responsibilities satisfied annual training requirements.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

CAMDBS' Compliance with Federal and Agency Security Requirements

We found that (1) OAR had developed and tested a contingency plan for CAMDBS and (2) personnel with significant security responsibility satisfied the Agency's recommended specialized security training necessary to perform their duties. However, we noted instances where OAR should place more emphasis to comply with established Federal and Agency information security requirements. In particular, our review noted:

- Although the CAMDBS system owner maintained a list of risks associated with the application, the system owner did not conduct a full formal risk assessment, which includes testing the controls as required by Federal and EPA requirements. Upon notification of our finding, OAR officials indicated that they entered POA&Ms in the Agency's security tracking database to track the completion of the risk assessment.

- One of the two CAMDBS production servers was not being monitored for known vulnerabilities. NCC personnel indicated that the server had been added to the routine vulnerability monitoring list and the Agency took immediate action to remediate the identified vulnerabilities.

Promptly conducting risk assessments and monitoring servers for security vulnerabilities help to assist managers in ensuring the Agency's network infrastructure is adequately protected. These widely recognized preventive controls aid in identifying potential security weaknesses and assist security personnel in taking the necessary remediation steps to prevent security incidents. By not emphasizing these key security controls, CAMDBS officials lacked key security management tools that could be used to proactively identify potential security weaknesses.

Certification and Accreditation

OAR could improve procedures to ensure that key security tasks are completed. Although OAR maintained a Risk Inventory and Assessment Table in the current security plan, OAR did not complete a full formal risk assessment to include testing the controls to ensure the controls were effective and operated as intended; 3 years had past since OAR last tested the controls. OAR officials indicated that they would complete the risk assessment. OAR also indicated that they have entered tasks in ASSERT to identify and track the requirements of incorporating National Institute of Standards and Technology Special Publication 800-53 *Recommended Security Controls for Federal Information Systems;* update the security plan; modify the C&A package; and obtain accreditation of CAMDBS by the end of September 2006.

The information used by OAR officials to make the reauthorization decision is contained in the CAMDBS C&A package, which includes documents such as the most recent system security plan, authorization for operation, and risk assessment. The assessment of risk is an important activity in the Agency's information security program that directly supports security accreditation (management's authorization to operate an information system). Maintaining an up-to-date C&A package is essential because senior OAR officials use these documents to determine whether CAMDBS' current security controls are sufficient and whether adjustments to security controls are necessary before reauthorizing CAMDBS and its subsystems to operate.

System Monitoring for Known Vulnerabilities

OAR security control processes did not ensure that all CAMDBS production servers were monitored for known vulnerabilities. The NCC manages the servers that run CAMDBS and provides the primary security controls for the application. Interviews with NCC personnel and vulnerability tests of the CAMDBS production servers revealed that one of the two CAMDBS production servers (1) was not being routinely monitored and (2) contained known vulnerabilities. Upon being notified of these weaknesses, NCC personnel informed us that the unmonitored server would be added to the routine vulnerability scanning list and the NCC took immediate action to remediate the identified vulnerabilities.

Routine monitoring of servers for vulnerabilities is widely recognized as a preventive control to assist security personnel in proactively identifying and eliminating commonly known threats before they can be exploited. With a formalized process to ensure this function is being performed, management has more assurance that OAR mission-critical information systems are adequately protected against publicized computer attacks.

Recommendations

We recommend that the Clean Air Markets Division Business System (CAMDBS) System Owner:

1. Conduct a full formal risk assessment of CAMDBS in accordance with Federal and Agency requirements.

2. Coordinate with the National Computer Center to verify that it is regularly monitoring all CAMDBS production servers for known vulnerabilities at least monthly.

3. Develop a Plan of Action and Milestones in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

We recommend that the Office of Air and Radiation (OAR) Information Security Officer:

4. Conduct a review of OAR's current information security oversight processes and implement identified process improvements.

Agency Comments and OIG Evaluation

OAR agreed with the findings in the draft report and indicated that the office has moved forward aggressively to implement the recommendations. OAR's complete response is in Appendix A.

Appendix A

Agency Response to Draft Report

April 24, 2006

MEMORANDUM

SUBJECT: Final Response to the OIG Draft Report on the 2005 CAMDBS Audit

FROM: Elizabeth Craig /s/
Deputy Assistant Administrator

TO: Rudolph M. Brevard, Director
Information Technology Audits
Office of the Inspector General

Thank you for the opportunity to review the revised draft report of the FY 2005 FISMA Audit of OAR's Clean Air Markets Division Business System (CAMDBS).

Attached is our response to the report and we agree with the findings and appreciate you bringing them to our attention. As you know, many of the minor problems were quickly resolved and activities are underway to address the remaining issues.

We look forward to seeing the final version, which should offer a balanced characterization of the identified problems.

cc: Brian McLean
Jerry Kurtzweg

April 20, 2006

Comments of OAR/OAP/Clean Air Markets Division
On the Findings and Recommendations in the
Revised OIG Final Audit Report,
"Information Security Series: Security Practices,
Clean Air Markets Division Business System, "
March 30, 2006

We have reviewed the revised Audit Report, "Information Security Series: Security Practices, Clean Air Markets Division Business System," Assignment No. 2005-000661, dated March 30, 2006. We concur with the findings and recommendations presented.

FINDINGS

Finding 1: CAMDBS is operating with an expired Risk Assessment.

We concur with this finding. The last full, formal, independent Risk Assessment for CAMDBS was completed in February 2002. We do understand and agree that "The assessment of risk is an important activity in the Agency's information security program [which] directly supports security accreditation (management's authorization to operate an information system)." This is, we believe, reflected by the fact that OAR has been performing annual risk assessments of CAMDBS through ASSERT. Nevertheless, a new full, formal, independent Risk Assessment should have been completed, triggered by the requirements for triennial review or major changes to the system. (Although the CAMDBS application itself was not changed significantly, there were changes in the underlying hardware when CAMDBS was moved from one data base server to another.)

As noted in the report, OAR did begin conducting a Risk Assessment in February 2005, and plans to complete the effort by the end of June 2006. This will result in certification and an updated Security Plan by early September 2006, and reaccreditation by the end of September 2006, when the current CAMDBS certification and accreditation would expire. (CAMDBS was last certified and accredited in October 2003.)

The delay in completing the Risk Assessment begun in 2005 was in response to an April 4, 2005 memorandum from the Deputy CIO, *Risk Based Decision to Temporarily Suspend the Requirement for Completion of Formal Risk Assessments to Support Security Plan Updates for Certain Systems*: "[T]his temporary suspension is … to allow for a reasonable, cost-effective transition to Agency-wide implementation of the new security life cycle being promulgated by the National Institute of Standards and Technology."

A Plan of Action and Milestones (POA&M) regarding the Risk Assessment was entered into ASSERT and is being tracked.

Finding 2: CAMDBS was operating without effective practices to ensure that all production servers were monitored for known security vulnerabilities.

We concur with this finding. We recognize that some technical vulnerabilities were identified in the OIG-performed scans of these systems and that coordination between CAMDBS and NCC staff needed improvement. Results of system scans have been shared with CAMDBS on an "exception" basis: problems requiring coordination were identified, but full results were not. We are working with NCC to develop a system of sharing system scan information that will meet both our needs. Staff and managers responsible for the operation and security profile of the CAMDBS application are in regular and frequent (at a minimum, biweekly, and usually, at the staff level, daily) contact with staff and managers at the NCC to discuss coordination and collaboration on matters of common interest and potential interaction and issue resolution.

Finding 3: OAR developed and tested a contingency plan for CAMDBS.

We concur with this finding. In fact, we believe that our efforts in this area are critically important and worthy of specific recognition.

Finding 4: Personnel with significant security responsibility completed the Agency recommended specialized security training

We concur with this finding.

RECOMMENDATIONS

We concur with all of the recommendations. In fact, we have moved ahead aggressively to implement these recommendations.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Air and Radiation
Acting Assistant Administrator for Environmental Information
Director, Technology and Information Security Staff
Audit Followup Coordinator, Office of Air and Radiation
Audit Followup Coordinator, Technology and Information Security Staff
Agency Followup Official (the CFO)
Agency Followup Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Acting Inspector General