OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Information Security Series: Security Practices

Integrated Contract Management System

Report No. 2006-P-00010

January 31, 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
EPA	Environmental Protection Agency
FISMA	Federal Information Security Management Act
ICMS	Integrated Contract Management System
OARM	Office of Administration and Resources Management
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-00010
January 31, 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 (EPA'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 Administration and Resources Management's (OARM's) Integrated Contract Management System (ICMS).

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. ICMS is the information system EPA uses to manage its contracts.

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/2006/20060131-2006-P-00010.pdf

Information Security Series: Security Practices Integrated Contract Management System

What We Found

OARM should place greater emphasis on key information system security practices to comply with Federal and Agency information security requirements. Specifically, we found that OARM's ICMS, a major application, was operating without (1) current certification and accreditation, (2) contingency plans or testing of the plans, and (3) a process to monitor servers for known security vulnerabilities. OARM officials could have discovered these noted deficiencies had they implemented procedures to ensure that Federal and Agency information security policies and guidelines were followed. As a result, ICMS had security vulnerabilities, which, if exploited, could have had a serious adverse effect on operations, assets, and individuals.

What We Recommend

We recommend that the OARM Information Security Officer:

- Develop a contingency plan for ICMS and implement a process to ensure the plan is tested at least annually,
- Implement processes to ensure ICMS production servers are periodically monitored for known vulnerabilities,
- Develop a Plan of Action and Milestone in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies, and
- Develop and implement a plan to re-evaluate system security oversight processes to ensure the above recommendations are uniformly applied to all general support systems and major applications within OARM.

OARM agreed with the report's findings and has indicated that the office has updated key security documents and started to address several of the identified issues. OARM maintains that the office has processes to ensure that ICMS servers it controls are monitored for known vulnerabilities. The office indicated many of the Office of Inspector General's concerns would be addressed when OARM finalizes its server consolidation project.

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

OFFICE OF
INSPECTOR GENERAL

January 31, 2006

MEMORANDUM

SUBJECT: Information Security Series: Security Practices
Integrated Contract Management System
Report No. 2006-P-00010

FROM: Rudolph M. Brevard, Director /s/
Information Technology Audits

TO: Luis A. Luna
Assistant Administrator for
Administration and Resources Management

This is our final report on the information security controls audit of the Office of Administration and Resources Management's Integrated Contract Management System conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This audit report contains findings that describe problems the 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 EPA position. EPA managers, in accordance with established EPA audit resolution procedures, will make final determinations on matters in this audit report.

Action Required

The Office of Administration and Resources Management does not have to provide a response to this report. The Agency's response to the draft report contained an adequate corrective action plan with milestone dates to implement the plan. Accordingly, we are closing this report on issuance. 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 have any questions regarding this report, please contact me at (202) 566-0893.

Table of Contents

Appendices

Purpose of Audit

Our objective was to determine whether the Office of Administration and Resources Management's (OARM's) Integrated Contract Management System (ICMS) complied with Federal and Agency information system security requirements. ICMS automates the Environmental Protection Agency's (EPA's) Federal acquisition and contract management processes. It generates solicitations, contract documents, purchase orders, contract modifications, and tasking documents.

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 that the security of its network infrastructure is consistent with these requirements. Program offices are responsible for managing the implementation of these security requirements within their respective organizations.

Program offices should create a Plan of Action and Milestone (POA&M) when they identify security control weaknesses. The POA&M, which documents the planned remediation process, is recorded in the Agency's Automated Security Self-Evaluation and Remediation Tracking (ASSERT) tool, which is used to centrally track remediation of weaknesses associated with Information Technology systems. ASSERT also 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*, issued October 3, 2005.

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*, issued October 17, 2005.

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 information security weaknesses identified in OARM. In particular, this report summarizes our results regarding how OARM's ICMS complies with Federal and EPA information security policies and procedures. This report also includes our evaluation of how OARM implemented, tested, and evaluated ICMS controls to ensure continued compliance with reviewed Federal and Agency requirements. The Scope and Methodology section contains the specific security objectives audited during this review.

Scope and Methodology

We conducted our field work from March 2005 to July 2005. Our primary location selected for review was the National Computer Center, Research Triangle Park (RTP), North Carolina. However, EPA uses ICMS in multiple locations other than RTP and we judgmentally selected two additional sites using the application – EPA Headquarters and Region 3.

We interviewed Agency officials at all locations and contract employees at the National Computer Center. We reviewed relevant Federal and Agency information security standards. We reviewed application security documentation and training records to determine whether they complied with selected standards. We reviewed system configuration settings and conducted vulnerability testing of servers for known vulnerabilities. We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

We assessed the adequacy of the following security practices for ICMS:

- **Security Certification and Accreditation (C&A) practices:** We reviewed ICMS' 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 Circular A-130 and EPA policy.

- **Application contingency plans**: We reviewed ICMS' contingency planning practices to determine whether they 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) physical controls, and (2) system vulnerability monitoring. We evaluated a sub-set of physical controls for selected ICMS server rooms at the EPA Headquarters and Region 3 offices. We did not test physical controls at RTP, because this location was undergoing an audit of these practices. The OIG found instances where EPA could improve its physical controls at RTP and reported the results 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*, issued December 14, 2005. We tested OARM's processes for monitoring the ICMS resources for known vulnerabilities, as required by Agency policy, and conducted vulnerability testing of all ICMS production servers at RTP, EPA Headquarters, and Region 3 offices.

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

ICMS' Compliance with Federal and Agency Security Requirements

Although we noted instances where ICMS was compliant with some Federal and Agency security requirements, our findings highlighted areas where OARM should place more emphasis to improve security practices surrounding ICMS and to better comply with established requirements. In particular, our review noted that ICMS contained security weaknesses in

- Timely updating and approving key C&A package documents,

- Developing and testing the contingency plan, and

- Monitoring the production servers for known vulnerabilities and mitigating high-risk vulnerabilities.

An effective security program helps offices coordinate, implement, and manage security-related activities and resources throughout the organization. Security practices that help ensure the Agency's network infrastructure is adequately protected include (1) preparing and maintaining an updated C&A package which documents the understanding and testing of implemented security controls necessary to operate an application, (2) documenting and testing the contingency plan to ensure the organization can recover from a disruption in service, and (3) monitoring servers for security vulnerabilities and verifying configuration settings to minimize exploitation from known threats.

By not providing emphasis in these areas, OARM places the integrity and availability of ICMS at greater risk. For example, our vulnerability test results

identified where ICMS servers contained weaknesses that would allow an intruder to (1) shut down the server and prevent legitimate user access to the system, or (2) modify confidential information in the ICMS database on the servers. Exploiting one of these vulnerabilities could result in reduced integrity of the data used by all EPA contracting offices for contract processing and degrade ICMS' availability, thereby hindering the contracting officers' ability to use the application to manage contractor tasking, allocation of funds, and contractor efforts. Further, due to the distributed nature of ICMS and the shared responsibility for security of the application and data, a security compromise at one or more locations could prevent OARM from obtaining an Agency-wide view of acquisition activity.

Certification and Accreditation

OARM should implement more comprehensive procedures to ensure that key C&A documents are prepared in a timely manner. The C&A package should include documents such as the most recent system security plan, authorization to operate, and the risk assessment. Although we did not find significant deficiencies with the ICMS risk assessment, our review revealed that the ICMS system owner did not prepare, update, and forward key security documents to senior OARM officials to reauthorize the system for continued operation. During field work, we found that ICMS had an outdated security plan and authorization to operate, which expired in March 2005 and February 2005, respectively. These key security documents are needed to determine whether ICMS' current security controls are sufficient, and if adjustments to security controls are necessary before reauthorizing ICMS for continued operation.

Upon bringing this issue to OARM's attention, personnel took action to remediate this deficiency and provided us an updated security plan and authorization to operate for ICMS.

Contingency Planning

OARM could improve its contingency planning for ICMS. OARM had not developed a plan for recovering or continuing operations of ICMS should a service disruption occur. Although OARM had established POA&Ms to develop and test a contingency plan, over several years, the program office took no action to develop a plan.

Contingency plans establish the necessary procedures for continuing operations for critical systems and applications following a disaster or loss of infrastructure support. Testing the plan would enable OARM to become familiar with the recovery steps and help OARM identify where additional emphasis is needed.

System Monitoring for Known Vulnerabilities

Although we found the physical controls adequate for the two sites we evaluated, OARM had not implemented processes to ensure that several ICMS servers were monitored for known vulnerabilities. Our results disclosed that OARM had not implemented monitoring for 55 percent (5 of 9) of the reviewed servers. As noted in Table 1, our tests discovered 50 unique, high-risk vulnerabilities on the reviewed servers. In addition, unmonitored servers had, on average, 70 percent more vulnerabilities than monitored servers.

Table 1. High Risk Vulnerabilities Discovered for Monitored Versus Unmonitored Servers

	Number of Servers	Number of Discovered Vulnerabilities	Average Number of Vulnerabilities per Server
Monitored	4	16	**4.0**
Unmonitored	5	34	**6.8**
Total	9	50	**-**

Note: *The total number of vulnerabilities does not include vulnerabilities identified as Medium or Low Risk or test results described as Informational. For password vulnerabilities, we counted one vulnerability per server, although the server may have had more than one instance of the same vulnerability.*

OARM shares responsibility with the regional offices for securing ICMS where the application operates. Ensuring all locations have implemented processes to routinely monitor servers for known security vulnerabilities and verifying the configuration of security settings helps reduce security incidents from occurring. With a formalized oversight process to ensure these functions are being performed, management would have greater assurance that OARM mission-critical information systems are adequately protected against known threats and computer attacks.

Recommendations

We recommend that the Office of Administration and Resources Management, Information Security Officer:

1. Develop a contingency plan for ICMS and implement a process to ensure the plan is tested at least annually.

2. Implement processes to ensure ICMS production servers are periodically monitored for known vulnerabilities.

3. Develop a POA&M in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

4. Develop and implement a plan to re-evaluate system security oversight processes to ensure the above recommendations are uniformly applied to all general support systems and major applications within OARM.

Agency Comments and OIG Evaluation

OARM concurred with many of the report's recommendations and outlined actions that would address several of the findings. However, OARM maintains that processes already exist to ensure that ICMS servers are periodically monitored for known vulnerabilities, citing on-going activities for servers under the direct control of OARM. As indicated above, OARM shares the responsibility for securing ICMS with the regional local area network managers operating the application. Agency policy indicates that the application owner is responsible for implementing processes to secure mission-critical applications. Although OARM may share the performance of the security responsibilities with the local area network managers, we believe the onus is with OARM, as the application owner, to implement an oversight process to ensure that security practices are implemented and effective.

OARM indicated that many of our concerns would be addressed once the office finalizes its server consolidation project. OARM indicated that this effort would bring ICMS' current distributed server architecture, spread out in the regional offices, to a centralized environment. OARM also provided additional information regarding the status of key ICMS security documents and the training status for personnel with significant security responsibilities. Where appropriate, we modified the report.

OARM's complete response is included as Appendix A.

Appendix A

Agency Response to Draft Report

MEMORANDUM

SUBJECT: Response to Draft Audit Report
Information Security Series: Security Practices
Office of Administration and Resources Management
Assignment No. 2005-000661

FROM: Luis A. Luna, Assistant Administrator /s/

TO: Rudolph M. Brevard, Director
Information Technology Audits

OARM appreciates the opportunity to respond to this Draft Audit Report. Our response is attached. We have already addressed several of the issues identified in the report. The security of OARM's information technology resources is a critical task that is taken very seriously.

If you or your staff has any questions, regarding the attached response, please contact Leo Gueriguian, OARM Information Management Official (IMO), at (202) 564-0388 or gueriguian.leo@epa.gov of my staff.

OARM Response to Draft Audit Report (Assignment No. 2005-000661)
December 20, 2005

The Office of Administration and Resources Management (OARM) respectfully submits the following responses to the Office of the Inspector General (OIG) regarding the audit report titled *Information Security Series: Security Practices, Office of Administration and Resource Management*, Assignment No. 2005-000661, dated December 2, 2005. This audit was conducted pursuant to the Federal Information Security Management Act (FISMA). The Integrated Contracts Management System (ICMS) was one of several EPA major applications reviewed in 2005 to meet FISMA requirements.

The following are the findings and recommendations made in the audit report and OARM's responses:

1. Certification and Accreditation (C&A)

OARM acknowledges that the ICMS security plan and authorization to operate were expired at the time of the Office of the Inspector General (OIG) audit. In addition, OARM concurs with the recommendation to update the security plan and authorization. This recommendation has already been completed.

The ICMS security plan was updated and approved June 30, 2005. A new Authorization to Operate memo was signed June 30, 2005. These documents were forwarded to OIG on July 5, 2005.

2. Contingency Planning

OARM acknowledges that ICMS does not have a final contingency plan. In September 2005, OARM developed a draft contingency plan and conducted a tabletop exercise. The contingency plan will be finalized as part of the Office of Acquisition Management's (OAM) server consolidation project. This effort will bring ICMS' current distributed server architecture, spread out in the Regional Offices, to a centralized environment. In the event of a service disruption, an alternate location shall provide the necessary ICMS functionality for the Agency. In addition, this solution will also place the entire ICMS operational environment under OARM's control, which will facilitate monitoring of security settings and testing for known vulnerabilities. We believe this effort, along with annual testing, will also satisfy the OIG recommendation to develop and test a contingency plan, with which OARM concurs. This plan will be completed by September 1, 2006.

3. System Monitoring for Known Vulnerabilities

OAM monitors production servers, under its control (RRB OAM server room, R6 and R9), on a daily basis. Monitoring is primarily for operational status, space availability, backup logs, console logs, and Oracle instances. Bindview reports are also run periodically, and Symantech anti-virus software runs on servers and desktops. In addition, Patchlink has been implemented on the desktops within OARM. OAM is in the process of developing a Change Management Process to assure that all OAM's infrastructure components have an appropriate, up to date security configuration. In conclusion, OARM feels that processes already exist to ensure that ICMS servers are periodically monitored for known vulnerabilities. Regardless, under the consolidated server project, OAM will have control of all ICMS servers and will be able to continue the system monitoring. The new system monitoring processes and change management process will be in place by September 1, 2006.

4. Security Training

The Office of Policy and Resources Management (OPRM) maintains overall management for the OARM IT security program. OPRM tracks and monitors the status of OARM staff's completion of required IT security training. Specifically, the Information Security Officer for OARM checks the status of the required training for OARM staff periodically throughout the year.

The Office of Environmental Information (OEI) maintains the US EPA Security Training database, which tracks the completion of required IT security training by EPA staff. For FY05, twelve OARM employees were

identified as having significant IT security responsibilities in this database. Three employees were incorrectly identified as having significant security responsibilities and did not need to take any additional training. All of the remaining nine OARM employees completed the required IT security training for FY05. Unfortunately, two staff members were incorrectly identified as not having completed the training in the database. In conclusion, all OARM employees with significant security responsibilities fulfilled the training requirement for FY05. The Information Security Officer (ISO) for OARM manages this required training program and will ensure that the tracking of this training will be accurate in the future.

Remaining recommendations

1. Develop Plans of Actions and Milestones, in the Agency's security weakness tracking system (ASSERT database), for all noted deficiencies.

OAM has an open Plan of Actions & Milestone (POA&M) for developing and documenting a log review process. POA&Ms will be created for revising and testing the Contingency Plan, to align this plan with the consolidated server environment, and for developing and documenting a Change Management Process for OAM's infrastructure.

2. Develop and implement a plan to re-evaluate system security oversight processes to ensure the above recommendations are uniformly applied to all general support systems and major applications within OARM.

For the specific findings with which OARM concurs, these issues are believed to be isolated occurrences, rather than a problem with overall security oversight processes. However, the ISO for OARM will conduct a review of OARM's major IT systems to validate that the recommendations of this report have already been completed. This review will be completed by March 31, 2006.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Administration and Resources Management
Regional Administrator, Region 3
Associate Director, Technology and Information Security Staff, Office of Environmental Information
Audit Followup Coordinator, Office of Administration and Resources Management
Audit Followup Coordinator, Region 3
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
Inspector General