OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Information Security Series: Security Practices

Comprehensive Environmental Response, Compensation, and Liability Information System

Report No. 2006-P-00019

March 28, 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
CERCLIS	Comprehensive Environmental Response, Compensation, and Liability Information System
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act
NCC	National Computer Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSWER	Office of Solid Waste and Emergency Response
POA&M	Plan of Action and Milestones
RTP	Research Triangle Park

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00019
March 28, 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 Comprehensive Environmental Response, Compensation, and Liability Information System (CERCLIS).

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. CERCLIS provides critical information in support of the Superfund program (a Federal mandate to clean up the Nation's uncontrolled hazardous waste sites).

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/2006/20060328-2006-P-00019.pdf

Information Security Series: Security Practices Comprehensive Environmental Response, Compensation, and Liability Information System

What We Found

The Office of Solid Waste and Emergency Response's (OSWER's) implemented practices to ensure production servers were being monitored for known vulnerabilities and personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that OSWER's CERCLIS, a major application, was operating without a current (1) certification and accreditation package and (2) contingency plan or testing of the plan. OSWER officials could have discovered the noted deficiencies had they implemented practices to ensure these Federal and Agency information security requirements were followed. As a result, CERCLIS had security control weaknesses that could effect OSWER's operations, assets, and personnel.

What We Recommend

We recommend that the CERCLIS System Owner:

- Conduct an independent review of security controls and a full formal risk assessment of CERCLIS and update the certification and accreditation package in accordance with Federal and Agency requirements,
- Conduct a test of the updated CERCLIS contingency plan, and
- 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 OSWER Information Security Officer:

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

OSWER agreed with the report's findings and has indicated that it has updated the CERCLIS security plan and re-authorized the application. OSWER officials also indicated that they updated the CERCLIS contingency plan and conducted a tabletop exercise of the updated plan. OSWER's complete response in included at Appendix A.

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

OFFICE OF
INSPECTOR GENERAL

March 28, 2006

MEMORANDUM

SUBJECT: Information Security Series: Security Practices
Comprehensive Environmental Response, Compensation, and Liability Information System
Report No. 2006-P-00019

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

TO: Susan Parker Bodine
Assistant Administrator for Solid Waste and Emergency Response

This is our final report on the information security controls audit of the Office of Solid Waste and Emergency Response's Comprehensive Environmental Response, Compensation, and Liability Information 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 have any questions regarding this report, please contact me at (202) 566-0893.

Table of Contents

At a Glance

Purpose of Audit 1

Background 1

Scope and Methodology 2

CERCLIS' Compliance with Federal and Agency Security Requirements 3

Certification and Accreditation 4
Contingency Planning 4

Recommendations 5

Agency Comments and OIG Evaluation 5

Appendices

A **Agency Response to Draft Report** 6

B **Distribution** 9

Purpose of Audit

Our objective was to determine whether the Office of Solid Waste and Emergency Response's (OSWER's) Comprehensive Environmental Response, Compensation, and Liability Information System (CERCLIS) complied with Federal and Agency information system security requirements. CERCLIS provides critical information and processing in support of the Superfund program (a Federal mandate to clean up the nation's uncontrolled hazardous waste sites).

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 Milestones (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) 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 from each of five EPA program offices and reviewed the security practices surrounding those applications. Our review noted instances where EPA could improve its security practices overall 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 practice weaknesses identified in OSWER. In particular, this report summarizes our results regarding how OSWER implemented Federal and EPA information security requirements. This report also includes our evaluation of how OSWER implemented, tested, and evaluated information security controls to ensure continued compliance with Federal and Agency requirements for selected security objectives. The Scope and Methodology section contains the specific security objectives we audited.

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) in 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 CERCLIS:

- **Security Certification and Accreditation (C&A) practices:** We reviewed CERCLIS' 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 CERCLIS' contingency planning practices to determine whether OSWER 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 identified two areas of security controls: (1) system vulnerability monitoring, which included conducting vulnerability testing; and (2) physical access controls. The NCC manages the servers that run the CERCLIS application and provides the primary security controls for the application. Therefore, when evaluating system vulnerability monitoring, we evaluated practices at the NCC. We did not test physical security controls at the NCC, because the NCC was undergoing an audit of these controls at the time of our review. This audit 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.

- **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.

CERCLIS' Compliance with Federal and Agency Security Requirements

We noted CERCLIS' production servers were being monitored for known vulnerabilities and personnel with significant security responsibility had completed the Agency's recommended specialized security training. However, our audit (1) disclosed that CERCLIS had deficiencies related to other significant security practices, and (2) highlighted areas where OSWER should place more emphasis to comply with established requirements. In particular, our review noted that CERCLIS contained security weaknesses in the following areas:

- The C&A package – consisting of a security plan, a third-party risk assessment, and a written authorization for operation – had not been updated in response to recent major system changes.

- The contingency plan had not been updated and tested in response to recent major system changes.

Preparing and maintaining an updated C&A package are vital in helping management determine whether effective security controls are in place and work as intended to operate an application. Updating and testing the contingency plan assist management in determining whether the organization could recover from a disruption in service. These two important security controls help ensure the Agency's network infrastructure is adequately protected. These widely recognized preventive controls aid in reducing the likelihood that security incidents will occur, and by not emphasizing these key security controls, OSWER places the integrity and availability of CERCLIS at risk. In response to these findings, OSWER officials indicated that they have updated the CERCLIS security and contingency plans and have conducted a tabletop exercise of the updated contingency plan.

Certification and Accreditation

Our audit revealed that the CERCLIS system owners had not updated the application security plan, risk assessment, and authorization for operation related to a recent major change in processing, as required by Federal and Agency policy. During our audit, we determined that CERCLIS had undergone a major change in processing. Specifically, CERCLIS changed from a decentralized application (distributed throughout EPA Headquarters and 10 EPA regional offices) to a centralized application (hosted by the NCC in RTP). However, we found that the CERCLIS security plan and risk assessment had not been updated, and the system had not been re-authorized for operation related to this "major change" in processing.

Senior OSWER officials use these key C&A security documents to make the decision about whether CERCLIS' security controls are sufficient and if adjustments to security controls are necessary before reaccrediting (reauthorizing) CERCLIS for continued operation. In addition, the assessment of risk and the development of system security plans are important activities in the Agency's information security program that directly support security accreditation (management's authorization for system operation). OSWER officials indicated that they have since updated CERCLIS' security plan to reflect these major system changes and re-authorized the application. OSWER also indicated that the CERCLIS Team Leader would make a determination when the next risk assessment is to be scheduled.

Contingency Planning

Although OSWER had developed and tested a contingency plan for CERCLIS, the program office had not updated the plan to reflect major changes made to the system. In audit Report No. 2006-P-00005, the OIG reported that CERCLIS' contingency plan did not identify critical resources needed during an outage. The OIG was unable to determine whether contracts were in place for the restoration of the application. In response to this finding, OSWER officials indicated that they conducted a tabletop exercise of CERCLIS in September 2005. However, OSWER officials did not indicate when the office would test the new plan.

Although OSWER conducted the tabletop exercise, Federal requirements specify that exercises and tests should be conducted to ensure that the procedures continue to be effective. In addition, testing of the plan would enable OSWER to become familiar with the necessary recovery steps and help management identify where additional emphasis is needed. OSWER officials indicated that the CERCLIS contingency plan had since been updated to reflect the changes to the application's operating environment and completed another tabletop review of the new plan in December 2005.

Recommendations

We recommend that the Comprehensive Environmental Response, Compensation, and Liability Information System (CERLIS) System Owner:

1. Conduct an independent review of security controls and a full formal risk assessment of CERCLIS and update the certification and accreditation package in accordance with Federal and Agency requirements,

2. Conduct a test of the updated CERCLIS contingency plan, and

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 Solid Waste and Emergency Response (OSWER) Information Security Officer:

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

Agency Comments and OIG Evaluation

OSWER concurred with many of the report's findings and indicated that the office took or planned steps to remediate the identified weaknesses. OSWER also provided additional details regarding its processes for maintaining the CERCLIS contingency plan and we modified the report to remove the recommendation to develop and implement a plan to maintain the contingency plan. OSWER also indicated that based on actions already taken, no further Plan of Action and Milestones are needed. However, given the resources required to complete the risk assessment and to test a contingency plan, we feel OSWER should record these significant security-planning activities in the Agency's security tracking system. OSWER's complete response is included as Appendix A.

Appendix A

Agency Response to Draft Report

March 2, 2006

MEMORANDUM:

SUBJECT: OSWER Response to Audit Report:
Information Security Series: Security Practices of the Comprehensive Environmental Response Compensation Liability Information System (CERCLIS)/Assignment No: 2005-000661

FROM: Susan Parker Bodine/s/
Assistant Administrator

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

Thank you for the opportunity to respond to the audit report on Information Security Series: Security Practices of the Comprehensive Environmental Response Compensation Liability Information System (CERCLIS). We appreciate your efforts to ensure the Agency is in compliance with the Federal Information Security Management Act (FISMA) by conducting annual audits of our applications. This memorandum addresses the accuracy of the audit report and identifies the corrective actions already initiated to ensure compliance.

RESPONSE TO RECOMMENDATIONS:

The system owner has provided the following information in response to your recommendations:

1. Update the CERCLIS certification and accreditation package in accordance with Federal and Agency requirements by ensuring that (1) the Security Plan is up to date, (2) an independent review of security controls and a full formal risk assessment are performed, and (3) management formally reauthorizes CERCLIS for operation.

The Security plan was updated and signed by the certifying official on 12/23/05 and by the authorizing official on 02/01/06.

The management, operational and technical security controls for the CERCLIS application are tested for effectiveness on a regular basis. The most recent review and independent tests for effectiveness of security controls were conducted by Booz Allen Hamilton, with a report delivered to EPA in February 2004. The risk assessment included documentation reviews,

manual and automated assessments of both computer hardware and software, which support the CERCLIS application. The risk assessment involved evaluating management, technical, and administrative controls already implemented. The elements of risk (threat, vulnerability, countermeasures, and impact) were evaluated as well.

In addition to the risk assessment, CERCLIS performs weekly and monthly reviews of all audit reports and logs. User accounts are reviewed quarterly to ensure accounts are valid. A determination is made regarding access to the system based on pre-determined roles and user/member groups. Accounts are reviewed to ensure users have taken the required annual security training. Accounts are deleted if they have not been active within ninety days. Consequences for violating access privileges and the Rules of Behavior are taken seriously; user ids are removed or suspended for violations. Quarterly reviews of management and operational controls are a part of the standard operating procedures for the CERCLIS application.

CERCLIS is moving away from performing a major risk assessment every three years to continuous monitoring of the application. Areas of focus are the management and control of its hardware, and performing security impact analysis. The agency has several IT security tools approved for use, licensed by EPA and available to Information Security Officers, System Administrators, and Local Area Network (LAN) Managers and Administrators to help protect IT assets. The CERCLIS Team Leader will make a determination when the next risk assessment is to be scheduled.

2. Conduct a test of the updated CERCLIS contingency plan.

OSRTI conducted the recommended test of the updated CERCLIS contingency plan on December 17, 2005.

3. Develop and implement a process to test and maintain the CERCLIS contingency plan. The process should ensure the plan is tested at least annually and that the plan is updated whenever significant changes occur to the system, supported business processes, key personnel, or to the contingency plan itself.

Over the past year, the Office of Superfund Remediation and Technology Innovation (OSRTI) has worked closely with EPA's National Computing Center (NCC) to centralize the CERCLIS Regional databases. As a follow-up to this work, the Contingency Plan for CERCLIS was revised in September 2005. Furthermore, a coordinated effort with the NCC has taken place to perform a table-top review of the CERCLIS application. The tabletop review was tested with participation and concurrence by the NCC on December 17, 2005. In complying with Agency standards, OSRTI has used the two National Institute of Standards and Technology (NIST) documents which focus specifically on contingency planning and testing. The first NIST document (NIST 800-84, Guide to Single-Organization IT Exercises) describes the procedures for the table-top review. The second document (NIST 800-34, Contingency Planning Guide for Information Technology Systems) describes in detail how to write a Contingency Plan.

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

Based on actions already taken as noted above, no further action is required because the noted deficiencies have been addressed.

5. 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 OSWER.

The OSWER Information Security Officer (ISO), in coordination with and supported by the Senior Information Official (SIO) and Information Management Officer (IMO), oversees a coordinated review of all OSWER systems annually with ongoing monitoring of major security milestones throughout the year. OSWER uses the Agency's ASSERT System to manage this process. Self-assessments occur annually and Plan of Actions and Milestones are generated to ensure changes or needed processes are addressed. OSWER's security status, as recorded in ASSERT, is independently audited by the Office of Environmental Information.

Please feel free to contact Robert King at 703.603.8792 or William Bushee at 703.603.8963, if you have any questions or need additional information.

cc: Renee Wynn
Kevin Phelps
Paula Rodriguez
Michael B. Cook
Joan Harrigan-Farrelly
Patricia Gowland

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Solid Waste and Emergency Response
Acting Assistant Administrator for Environmental Information
Acting Director, Technology and Information Security Staff
Audit Followup Coordinator, Office of Solid Waste and Emergency Response
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