OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Information Security Series: Security Practices

Safe Drinking Water Information System

Report No. 2006-P-00021

March 30, 2006

Report Contributors:

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

Abbreviations

ASSERT	Automated Security Self-Evaluation and Remediation Tracking Tool
C&A	Certification and Accreditation
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
OW	Office of Water
POA&M	Plan of Action and Milestones
RTP	Research Triangle Park
SDWIS	Safe Drinking Water Information System

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00021
March 30, 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 Water's (OW's) Safe Drinking Water Information System (SDWIS).

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. SDWIS supports EPA's initiative to protect public health by allowing EPA to provide a repository of national public drinking water data to interested stakeholders.

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/2006/20060330-2006-P-00021.pdf

Information Security Series: Security Practices Safe Drinking Water Information System

What We Found

We found that the Office of Water (OW) substantially complied with many of the information security controls reviewed and had implemented practices to ensure production servers are monitored for known vulnerabilities, physical access controls are adequate, and personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that the Safe Drinking Water Information System (SDWIS), a major application, did not have complete certification and accreditation documents. In addition, the contingency plan did not contain all elements specified by Federal and Agency requirements. OW officials could have discovered the identified weaknesses had the office reviewed its implemented practices for completing these requirements. As a result, SDWIS had security control weaknesses that could affect OW's operations, assets, and individuals.

What We Recommend

We recommend that the SDWIS System Owner:

- ➢ Complete the independent review of security controls, complete a full formal risk assessment of SDWIS, and update the certification and accreditation package.
- ➢ Update and test the SDWIS contingency plan and implement a process to periodically test and maintain the plan.
- ➢ 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 OW Information Security Officer:

- ➢ Conduct a review of OW's information security oversight processes.

OW agreed with the report's findings, indicated that it was in the process of completing the risk assessment, and expected to complete the assessment by the end of March 2006. OW also stated it would update and test the SDWIS contingency plan as a follow-up to the formal risk assessment. OW expressed concerns that some of the findings could give a misleading picture of the security of SDWIS at the time of our review and we updated the report to reflect efforts OW took to address the findings. OW's complete response is in Appendix A.

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

OFFICE OF
INSPECTOR GENERAL

March 30, 2006

MEMORANDUM

SUBJECT: Information Security Series: Security Practices
Safe Drinking Water Information System
Report No. 2006-P-00021

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

TO: Benjamin H. Grumbles
Assistant Administrator for Water

This is our final audit report on the information security controls audit of the Office of Water's Safe Drinking Water 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 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 me at (202) 566-0893.

Table of Contents

Appendices

Purpose of Audit

Our objective was to determine whether the Office of Water's (OW's) Safe Drinking Water Information System (SDWIS) complied with Federal and Agency information system security requirements. SDWIS supports EPA's initiative to protect public health by allowing EPA to provide a repository of national public drinking water data to interested stakeholders to enable them to monitor the quality of the Nation's drinking water.

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 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 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. 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 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*.

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 OW. In particular, this report summarizes our results regarding how OW implemented

Federal and EPA information security policies and procedures. This report also includes our evaluation of how OW 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), 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.

During the audit, OW was operating two production versions of SDWIS:

- SDWIS-current, a mainframe-based application hosted at the NCC in RTP, North Carolina; and

- SDWIS-modern, a Web-enabled, tiered application also hosted at the NCC in RTP, North Carolina.

OW replaced SDWIS-current with the SDWIS-modern system. When OW placed the SDWIS-modern system into production, the office operated it in parallel with the SDWIS-current application. We only evaluated the SDWIS-modern application for compliance with Federal and Agency requirements and all references to SDWIS, in this report, pertain to the SDWIS-modern application.

We assessed the following security practices for SDWIS:

- **Security Certification and Accreditation (C&A) practices** -- We reviewed SDWIS' 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 SDWIS' contingency planning practices to determine whether it 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 access controls. OW operates SDWIS servers in its Washington, DC, Headquarters and at the NCC in RTP. At the Headquarters office, we evaluated the location for both system vulnerability monitoring and physical access controls. At the NCC, we only evaluated system vulnerability monitoring. We did not evaluate physical access controls at the NCC, because the NCC was undergoing an audit of these controls at the time of our review. This audit identified instances where EPA could improve its physical controls at RTP and the OIG 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.*

- **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.

SDWIS' Compliance with Federal and Agency Security Requirements

The SDWIS production servers were being monitored for known vulnerabilities, physical access controls were adequate, and personnel with significant security responsibility had completed the Agency's recommended specialized security training. Our audit (1) noted that SDWIS had weaknesses related to key security practices, and (2) highlighted areas where OW should place more emphasis to comply with established information security requirements. OW officials could have discovered these weaknesses had they implemented procedures to ensure that Federal and Agency information security requirements were followed. In particular, SDWIS had the following information security planning weaknesses:

- The C&A package did not contain a completed independent review of SDWIS' security controls and a completed full formal risk assessment.

- The contingency plan did not contain fully developed essential elements identified by Federal and Agency guidance and was not tested.

Preparing and maintaining updated C&A documents and contingency plans help to 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, OW places the integrity and availability of SDWIS at risk. In addition, testing these controls provides management with assurance that the controls are adequately implemented and working as intended. For example, an inadequately designed security control could result in a breach in SDWIS' security and result in reduced system availability or affect the integrity of the system's data. This could hinder the ability of Federal officials and other stakeholders to use SDWIS to monitor the quality of the Nation's drinking water.

Certification and Accreditation

We found areas where OW could implement more comprehensive procedures to ensure C&A documents are complete. Specifically, the system owners had not conducted an independent review of SDWIS' security controls and performed a full formal risk assessment of SDWIS prior to authorizing the application for operation as required by Federal and Agency guidance.

The information used by OW officials to make the initial authorization decision is contained in the SDWIS C&A package, which includes documents such as the most recent system security plan, authorization for operation, test of implemented security controls, and risk assessment. These documents support the OW risk management process and are necessary for senior OW officials to decide whether SDWIS' security controls are sufficient, and if adjustments to security controls are necessary before authorizing SDWIS for operation.

During our audit, OW was conducting a Capital Planning and Investment Control review of SDWIS. OW officials indicated that the review highlighted the need to conduct a risk assessment, and to prepare and implement a risk management plan for all aspects of SDWIS. OW officials indicated an assessment would identify weaknesses that need to be addressed, and that they will address these through a process of defining each weakness and establishing a POA&M to deal with each one. OW officials indicated the risk assessment would be completed in March 2006.

Contingency Planning

We found that OW could improve its contingency planning procedures for SDWIS. Although OW had included a contingency planning section in the SDWIS security plan, OW had not fully developed the plan to include essential elements that make up an effective contingency plan as outlined in Federal and Agency guidance. In addition, OW had not conducted a test of the contingency planning procedures outlined in the security plan. OW stated that they would update and test the SDWIS contingency plan as a follow-up to the formal risk assessment performed during March 2006.

An effective contingency plan should include Supporting Information, a Notification/activation phase, a Recovery Phase and a Reconstitution phase. Federal and EPA standards require that plans be (1) reviewed and tested annually, and (2) updated as necessary when changes in business needs, technology, or new internal or external policies occur. Testing the plan would enable OW to become familiar with the recovery steps and help management identify where additional emphasis is needed.

Recommendations

We recommend that the Safe Drinking Water Information System (SDWIS) System Owner:

1. Complete the independent review of SDWIS' security controls, complete a full formal risk assessment of SDWIS, and update the certification and accreditation package in accordance with Federal and Agency requirements.

2. Update and test the SDWIS contingency plan in accordance with Federal and EPA requirements; implement a process to test the plan annually; and update the contingency plan whenever significant changes occur to the system, supported business processes, key personnel, or the contingency plan itself.

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 Water (OW) Information Security Officer:

4. Conduct a review of the information security oversight processes within OW and develop and implement a plan to implement needed process improvements.

Agency Comments and OIG Evaluation

The Office of Water (OW) agreed with our finding that the Safe Drinking Water Information System (SDWIS) had not undergone a risk assessment and the office indicated that it has plans to complete the assessment. OW did not agree that SDWIS' security plan did not accurately reflect the system's appropriate operational status, citing differences between how OW and the EPA's Chief Information Officer define a "production" system. OW contends that at the time of our review, SDWIS did not have substantiated data in the system and provided additional detail regarding SDWIS' implementation. We modified the report to update the section related to SDWIS' operational status and to reflect efforts OW took to address the findings.

OW did not agree with our finding that SDWIS did not have a contingency plan and provided additional information on the system's plan. Although OW documented some contingency planning information, our research disclosed that the information provided was not fully developed as required by Federal and Agency requirements. OW's complete response is in Appendix A.

Appendix A

Agency Response to Draft Report

MEMORANDUM

SUBJECT: Draft Audit Report Information Security Series: Security Practices
Safe Drinking Water Information System
Assignment No. 2005-000661

FROM: Benjamin H. Grumbles
Assistant Administrator, Office of Water

TO: Rudolph M. Brevard
Director, Information Technology Audits

Thank you for the opportunity to respond to the draft Audit Report on Security Practices pertaining to the Safe Drinking Water Information System (SDWIS). While we found your review instructive relative to the requirements of the Federal Information Security Management Act (FISMA), we believe that your draft Audit Report gives a misleading picture of the security of SDWIS at the time of your review.

At the time of your review, the Office of Water (OW) had in place approved security plans consistent with the status of the various system components. As you know, OW has been modernizing the entire SDWIS data flow since 2001, and that modernization was still underway at the time you conducted your review. Key points that I believe conflict with your office's evaluation include:

> Even though SDWIS/Federal (the system in use at the time of your review) and SDWIS/Operational Data System (ODS) (the system under development) were operating in parallel, the data in SDWIS/ODS were test data and were not available to the public, peers, educational institutions or other federal agencies. These data were strictly for test purposes, and were maintained in separate test environment. Hence the SDWIS/ODS was under development as described in the OW security plan.
>
> OW defines "production" differently than the Office of Environmental Information (OEI). OEI defines a system as in "production" when the relevant server is connected to the network. However, OW does not consider a system to be in production until we have substantiated data that we can provide to our peers. In the case of SDWIS/ODS, at the time of your review, OW did not have substantiated data in the system, and thus we did not consider the system to be in production.
>
> The SDWIS security plan in place at the time of your review appropriately covered SDWIS in its status of "under development, and included a contingency planning process.

I would also like to note that at the time of your review, OW was also responding to the Office of Management and Budget's Capital Planning and Investment Control (CPIC) review of SDWIS. The CPIC review highlighted the need to conduct a risk assessment, and to prepare and implement a risk management plan for all aspects of SDWIS. We are in the process of completing that assessment now and expect to be finished in March 2006. In addition, as required by FISMA, OW has been conducting a self-assessment of SDWIS. The results of this self assessment will be documented in the Agency's Automated Security Self Evaluation and Remediation Tracking (ASSERT) system. Along with the self-assessment, Plans of Actions and Milestones will be documented in ASSERT. OW expects to complete this effort by the end of March 2006. The information in ASSERT will be used by OW for continuous monitoring of the overall security of SDWIS, in keeping with the use of ASSERT as the Agency's standard for implementing continuous security self-assessments. For example, OW undertakes tabletop exercises, and documents the results of those exercises in ASSERT, as part of our annual contingency planning.

We look forward to continuing to work with you and your staff on these important issues. We will also be sending you under separate cover a more detailed set of technical comments for your consideration. If you or your staff have any questions regarding this response, please contact Steve Heare, Director, Drinking Water Protection Division, at 202-564-7992 or Terry Howard, OW Information Security Officer, at 202-564-0385.

Appendix B

Distribution

Office of the Administrator
Assistant Administrator for Water
Acting Assistant Administrator for Environmental Information
Acting Director, Technology and Information Security Staff
Audit Followup Coordinator, Office of Water
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