OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

Information Security Series: Security Practices

Integrated Compliance Information System

Report No. 2006-P-00020

March 29, 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	U.S. Environmental Protection Agency
FISMA	Federal Information Security Management Act
ICIS	Integrated Compliance Information System
NCC	National Computer Center
OECA	Office of Enforcement and Compliance Assurance
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
RTP	Research Triangle Park

U.S. Environmental Protection Agency
Office of Inspector General

2006-P-00020
March 29, 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 Enforcement and Compliance Assurance's (OECA's) Integrated Compliance Information System (ICIS).

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. ICIS provides critical data and processing in support of the Agency's environmental law enforcement and compliance program.

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/2006/20060329-2006-P-00020.pdf

Information Security Series: Security Practices Integrated Compliance Information System

What We Found

The Office of Enforcement and Compliance Assurance (OECA) had implemented practices to ensure that the (1) Integrated Compliance Information System (ICIS) production servers were monitored for known vulnerabilities and (2) personnel with significant security responsibility completed the Agency's recommended specialized security training. However, we found that OECA could improve its practices to ensure that key security documents are maintained. Additionally, ICIS, a major application, was operating without a contingency plan or testing of the plan. OECA officials could have discovered the noted deficiencies had they implemented processes to ensure these Federal and Agency information security requirements were followed. As a result, ICIS had security control weaknesses that could affect OECA's operations, assets, and individuals.

What We Recommend

We recommend that the ICIS System Owner:

- Conduct a review of processes used to maintain ICIS' key information security documents and implement identified process improvements,
- Conduct a test of the ICIS contingency plan, and
- Develop Plans of Action and Milestones (POA&Ms) in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

We recommend that the OECA Information Security Officer:

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

OECA agreed that ICIS needed a contingency plan and the office developed a plan. OECA did not agree that ICIS' security plan was not up-to-date, the office should create a plan to review its information security practices, and POA&Ms are needed for the identified weaknesses. Our audit disclosed that key security documents were not updated to reflect the results of critical security activities and although OECA developed a contingency plan, the office has not tested it. As such, OECA should re-evaluate its security oversight program to identify weaknesses and create POA&Ms to track remediation of uncompleted tasks. OECA's response is at Appendix A.

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

OFFICE OF
INSPECTOR GENERAL

March 29, 2006

MEMORANDUM

SUBJECT: Information Security Series: Security Practices
Integrated Compliance Information System
Report No. 2006-P-00020

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

TO: Granta Nakayama
Assistant Administrator for Enforcement and Compliance Assurance

This is our final audit report on the information security controls audit of the Office of Enforcement and Compliance Assurance's Integrated Compliance 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, or Charles Dade, Assignment Manager, at (202) 566-2575.

Table of Contents

Appendices

Purpose of Audit

Our objective was to determine whether the Office of Enforcement and Compliance Assurance's (OECA's) Integrated Compliance Information System (ICIS) complied with Federal and Agency information security requirements. ICIS provides critical data and processing in support of the Agency's environmental law enforcement and compliance program.

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) 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 OECA. In particular, this report summarizes our results regarding how ICIS complies with Federal and EPA information security policies and procedures. This report also

includes our evaluation of how OECA implemented, tested, and evaluated ICIS' information security controls to ensure continued compliance with reviewed Federal and Agency 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 all 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 assessed the following security practices for ICIS:

- **Security Certification and Accreditation (C&A) practices --** We reviewed ICIS' 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 ICIS' 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. The NCC manages the servers that run ICIS 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. We 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.

ICIS' Compliance with Federal and Agency Security Requirements

We noted ICIS' 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 highlighted areas where OECA should place more emphasis to comply with established Federal and Agency requirements. In particular, ICIS had weaknesses in the following areas:

- The practices for maintaining the security plan could be improved. The application security plan did not reflect ICIS' current operational status or document key security planning activities.

- The application lacked a contingency plan or testing of contingency response.

Ensuring effective practices for updating and maintaining the application security plan is vital in helping management determine whether effective security controls are implemented and operate as intended to operate an application. Developing and testing the contingency plan assist management in evaluating whether the organization can recover from a disruption in service and determine where more emphasis is needed. These two important and widely recognized preventive controls help to protect the Agency's network infrastructure and assist EPA personnel to respond effectively to security incidents. By not emphasizing these key security controls, OECA places the integrity, confidentiality, and availability of ICIS information at risk.

Certification and Accreditation

Although we did not find significant deficiencies with the ICIS risk assessment and authorization to operate, our audit revealed that OECA practices for maintaining the security plan could be improved to ensure key security information is updated and key security activities are recorded. Our review determined that:

- The security plan OECA provided for review did not accurately reflect ICIS' current operational status. Although OECA officials indicated that they updated the security plan twice since ICIS' implementation in

June 2002, the security plan OECA submitted for review indicated ICIS was under development.

- The security plan OECA provided for review did not reflect key security planning activities. OECA officials indicated that the security plan was updated in July 2004 and again in September 2004 because of a Risk Assessment and Vulnerability Assessment, respectively. However, these key security-planning activities were not recorded in the security plan OECA officials submitted for review.

Ensuring that effective practices are in place to ensure the security plan is up-to-date is essential. The security plan is a key document used by senior OECA officials to decide whether ICIS' current security controls are sufficient and whether adjustments to security controls are necessary before reaccrediting (reauthorizing) ICIS for continued operation.

Contingency Planning

OECA should improve its contingency planning for ICIS. OECA had not developed a plan for recovering or continuing operations of ICIS should a service disruption occur. Contingency plans establish the necessary procedures for continuing operations for critical systems and applications following disasters or loss of infrastructure support. Testing the plan would enable OECA to become familiar with the necessary recovery steps and help management identify where additional emphasis is needed.

OECA officials indicated that the office had developed a contingency plan for ICIS. OECA officials indicated that the contingency plan would be reviewed, revised, and re-approved in fiscal 2006 due to the implementation of ICIS Phase II. OECA officials indicated that they are investigating a more robust disaster recovery process, scheduled to be completed by the end of fiscal 2006. In this regard, OECA should record these key activities and milestones in the Agency's security weakness system (ASSERT database) for tracking.

Recommendations

We recommend that the Integrated Compliance Information System (ICIS) System Owner:

1. Conduct a review of processes used to maintain ICIS' key information security documents and implement identified process improvements.

2. Conduct a test of the ICIS contingency plan.

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 Enforcement and Compliance Assurance's (OECA's) Information Security Officer:

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

Agency Comments and OIG Evaluation

OECA agreed with our finding that ICIS lacked a contingency plan and OECA officials indicated that they took action to remediate the weakness. However, OECA should put in place a strategy for testing the new contingency plan. OECA did not agree that ICIS' security plan was not up-to-date and indicated that subsequent to our audit field work the office updated the security plan, and we modified the report to remove the recommendation for OECA to update the ICIS security plan.

OECA asserts that it has adequate practices in place for maintaining the security plan and overseeing the program office's security program. OECA indicated that it reviews and recertifies all security plans for major applications every three years, as well as when a significant change to the application has occurred and annually tests and evaluates information security controls and techniques, tracks the remediation of information security weaknesses identified, and reports the status of information security. However, our audit revealed that despite these efforts, OECA's oversight practices did not ensure the security plan was (1) updated with ICIS' current operational status and (2) reflected the results of key security activities. Additionally, OECA's practices did not ensure that ICIS, a major application, had an effective contingency plan or strategy, although the application had been in production for 3-years. Therefore, we feel OECA should re-evaluate its information security oversight processes to identify opportunities where information security could be strengthened.

OECA indicated that no further POA&Ms are needed to address the identified weaknesses. OECA indicated it has plans for major contingency planning activities for ICIS and the office is in the process of investigating and evaluating a more robust disaster recovery process. OECA also has not completed a test of the newly developed contingency plan. In this regard, OECA should record these key activities and milestones in the Agency's security weakness database (1) for tracking and (2) to keep the Agency's CIO informed about the mitigation of security weaknesses for a key EPA major application. OECA's complete response is at Appendix A.

Appendix A

Agency Response to Draft Report

March 9, 2006

MEMORANDUM

SUBJECT: Response to Draft Report "EPA Could Improve Information Security Practices for the Integrated Compliance Information System"

FROM: Granta Y. Nakayama /s/
Assistant Administrator

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

On February 9, 2006, the Office of Enforcement and Compliance Assurance (OECA) received the Office of Inspector General (OIG) draft report memorandum titled, "EPA Could Improve Information Security Practices for the Integrated Compliance Information System". In response to your draft report, provided below is additional information that more accurately reflects the state of our Information Security Practices as of the time of the writing of your report. OECA appreciates the opportunity to respond to this draft report and hopes that you will take into consideration the information provided when finalizing your report.

Response or Actions Taken to Address OIG Recommendations

1. *Update the ICIS Security Plan.*

OECA disagrees with your finding that the Integrated Compliance Information System (ICIS) Security Plan was not up to date at the time of your audit. ICIS currently has in place an updated Security Plan. The original ICIS Security Plan was approved in April 2002, prior to the system going into operation. ICIS was implemented on June 22, 2002. In November 2002, a review was conducted pursuant to the OMB A-130 requirement that security plans be reviewed subsequent to a significant change in the application. The deployment from the development environment to the production environment was deemed by the Office of Compliance ISO to be such a significant change. The revised ICIS Security Plan was approved on November 27, 2002. In December 2003, an ICIS Risk Assessment was performed to test the controls within the Security Plan. The Security Plan was updated in July 2004 to incorporate recommendations from the Risk Assessment. A Technical Vulnerability Assessment of ICIS was performed in

September 2004. The plan was then again revised in April 2005 to incorporate recommendations from the Vulnerability Assessment. In July 2005 the plan was updated to meet new formatting requirements from NIST 800-18. On July 28, 2005, the ICIS Security Plan was re-approved, and the ICIS system was reauthorized to operate per requirements of OMB Circular A-130 and EPA policy. As a result, OECA believes we have already completed work to comply with this recommendation.

2. Develop and implement a process to periodically review and maintain the ICIS security plan in accordance with Federal and Agency requirements.

OECA currently has processes in place to periodically review and maintain the ICIS Security Plan. In accordance with OMB A-130 Appendix III, OECA reviews and recertifies all security plans for major applications every three years, as well as when a significant change to the application has occurred. It is for the latter reason that the security plan dated July 28, 2005, is now being revised, following NIST 800-53 guidelines in preparation for the deployment of ICIS Phase II. The draft revised plan is in the review and comment process and will be approved prior to the implementation of the second phase of ICIS this fiscal year.

In addition, as required under the Federal Information Security Management Act of 2002 (FISMA), OECA annually tests and evaluates information security controls and techniques, tracks the remediation of information security weaknesses identified, and reports the status of information security. The ASSERT (Automated Security Self-Evaluation & Remediation Tracking) tool is used to automate this process. The combination of this annual process and regular review and re-approval of the Security Plan ensures that the ICIS Security Plan and procedures are kept up-to-date as required by Federal and Agency requirements.

3. *Develop and implement a contingency plan for ICIS.*

OECA has developed and has in place a contingency plan for ICIS. That plan was reviewed based on Disaster Recovery Institute International (DRII) standards and was approved as of February 6, 2006. The ICIS Contingency Plan provides the following information: a business impact analysis, which assesses the value of the ICIS information; emergency procedures for limited, major, and catastrophic disruptions to ICIS; and recovery plans and testing requirements.

4. Develop and implement a process to test and maintain the ICIS contingency plan. The process should ensure the plan is (1) tested at least annually and (2) updated whenever significant changes occur to the system, supported business processes, key personnel, or to the contingency plan itself.

The contingency plan will be reviewed, revised and re-approved in FY2006 because of significant changes to the system resulting from the implementation of the ICIS Phase II system. ICIS Phase II will replace the current ICIS system and will greatly expand the current data and functionality of the system. In addition, OECA is in the process of investigating and evaluating a more robust disaster recovery process. This investigation includes reviewing the current

approach and considering more efficient alternatives for disaster recovery. These activities are scheduled to be complete by the end of FY2006. In FY2007, OECA's plan is to review and update the ICIS Contingency Plan to incorporate results from the disaster recovery investigation. Now that the Contingency Plan is in place, it is a part of OECA's annual testing and evaluation of information security controls and techniques where we track the remediation of information security weaknesses identified, and report the information security status. As a result of our using processes currently in place, OECA believes we already comply with this recommendation.

5. Develop Plans or Action and Milestones in the Agency's security weakness tracking system (ASSERT database) for all noted deficiencies.

ICIS security weaknesses identified through the annual self-assessment result in Plans of Action and Milestones (POA&Ms) are being created and tracked through ASSERT. There are currently no open POA&Ms in ASSERT for ICIS. In addition, because all of the findings of this report have been addressed per OECA's responses, no additional POA&Ms are required to be tracked.

6. 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 OECA.

The OECA and Office of Compliance Information Security Officers (ISOs) currently have procedures in place that ensure that they regularly review security checklists to make sure that all government wide and Agency requirements are met in a timely manner. Given the additional information provided in this response, we feel that current oversight processes are adequate to ensure that OECA systems remain in compliance with security policy.

If you need any additional information, please contact Betsy Smidinger, Deputy Director of the Enforcement Targeting and Data Division on OECA's Office of Compliance, at 202-564-4017 or at email address smidinger.betsy@epa.gov.

cc: Catherine McCabe
Linda Travers
Michael Stahl
Carolyn Sanders
Gwendolyn Spriggs
Kathy Dockery

Appendix B

Distribution

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