OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Audit Report

EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance

Report No. 2007-P-00017

March 29, 2007

Report Contributors: Rudolph M. Brevard
Chuck Dade
Corey Costango
Sejal Shah

Abbreviations

BAS	Budget Automation System
CSIRC	Computer Security Incident Response Capability
DBMS	Database Management System
EPA	U.S. Environmental Protection Agency
FDW	Financial Data Warehouse
IFMS	Integrated Financial Management System
ISO	Information Security Officer
IRMS	Integrated Resource Management System
NIST	National Institute for Standards and Technology
OCFO	Office of the Chief Financial Officer
OEI	Office of Environmental Information
OIG	Office of Inspector General
OPPIN	Office of Pesticide Programs Information Network
ORD	Office of Research and Development
OTOP	Office of Technology Operations and Planning
SLATE	Strategic Leasing and Asset Tracking Enterprise

U.S. Environmental Protection Agency
Office of Inspector General

2007-P-00017
March 29, 2007

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

We sought to determine whether the U.S. Environmental Protection Agency (EPA) (1) implemented and maintained database hardware and software in accordance with EPA policy requirements; and (2) secured critical financial information by restricting access to high-level database functions, such as database administrator authorities.

Background

EPA's core financial application, the Integrated Financial Management System (IFMS), shares data with many financial management system databases. An inadequately designed and implemented security control could be more easily breached, which could compromise the integrity of the data IFMS uses for financial reporting and decisionmaking.

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/2007/20070329-2007-P-00017.pdf

EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance

What We Found

We discovered weaknesses in how EPA offices (1) monitor databases for known security vulnerabilities, (2) communicate the status of critical system patches, and (3) monitor the use of and access to database administrator accounts and privileges. These weaknesses exist because EPA had not implemented security processes to (1) actively monitor systems that share data with IFMS, (2) share and collect information on the implementation of critical system patches, and (3) effectively manage access controls. Without these processes, the integrity of critical data in key Office of the Chief Financial Officer (OCFO) systems could be undermined. As a result, OCFO cannot ensure that the integrity of the data it provides to senior Agency officials is adequately protected.

We also identified specific technical weaknesses in three of the financial databases that share data with IFMS.

What We Recommend

We recommend that OCFO, the Office of Environmental Information (OEI), and the Office of Research and Development address areas where EPA could improve. Specifically, we recommend that:

- OCFO update the Memorandum of Understanding process to include formal security standards that require the program/regional offices to actively monitor the security status of systems that share data with IFMS.
- OEI strengthen, formalize, and evaluate the effectiveness of the followup procedures for obtaining complete responses from program and regional offices regarding high-level critical system patch alerts, as well as share status reports on the implementation of critical system patches.
- The system owners for each reviewed application correct all identified system weaknesses, and develop a Plan of Action and Milestones in the Agency's security weakness tracking system for all noted deficiencies.

The Agency agreed with all of our recommendations.

Due to the sensitive nature of the report's technical findings, we removed Appendices A, C, and D from the public version of the report.

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

OFFICE OF
INSPECTOR GENERAL

March 29, 2007

MEMORANDUM

SUBJECT: EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance
Report No. 2007-P-00017

FROM: Patricia H. Hill
Assistant Inspector General for Mission Systems

TO: Lyons Gray
Chief Financial Officer

Molly A. O'Neill
Assistant Administrator for Environmental Information

George M. Gray, Ph.D.
Assistant Administrator for Research and Development

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The estimated cost of this report – calculated by multiplying the project's staff days by the applicable daily full cost billing rates in effect at the time – is $356,118.

Action Required

In accordance with EPA Manual 2750, the Office of the Chief Financial Officer is required to provide a written response to this report within 90 calendar days. You should include a corrective action plan for agreed upon actions, including milestone dates.

The Office of Environmental Information and Office of Research and Development do not have to provide a response to this report. The offices' response to the draft report contained an adequate corrective action plan with milestone dates to address the recommendations. Accordingly, we are closing this report on issuance.

Due to the sensitive nature of the technical findings, we have removed Appendices A, C, and D from the report version made available to the public. The public copy of this report will be available at http://www.epa.gov/oig. Additional copies of the full report can be obtained by contacting our Office of Congressional and Public Liaison at (202) 566-2391.

If you or your staff has any questions, please contact me at 202-566-0894 or hill.patricia@epa.gov; or Rudolph M. Brevard, Director, Information Resources Management Assessments, at (202) 566-0893 or brevard.rudy@epa.gov.

Table of Contents

Chapters

Appendices

Chapter 1
Introduction

Purpose

We completed this audit to determine whether the U.S. Environmental Protection Agency (EPA) (1) implemented and maintained database hardware and software in accordance with EPA policy requirements; and (2) secured critical financial information by restricting access to high-level database functions, such as database administrator authorities.

Background

The Integrated Financial Management System (IFMS) is EPA's core financial management accounting system. IFMS (1) supports the standard general ledger, (2) is the source of data for preparing financial statements and budgetary reports, and (3) supports program offices in managing and controlling funds. IFMS depends heavily upon data processed by many other systems in order to provide senior Agency officials with timely and accurate information. Although the Office of the Chief Financial Officer (OCFO) is the IFMS system owner, many of the financial management systems that share data with IFMS are managed by other program offices. Therefore, OCFO must coordinate the implementation of security controls between offices to protect the integrity of shared data.

OCFO must implement a security program that is consistent with EPA's current security philosophy. Currently, EPA distributes the implementation and management of information security to multiple organizations. Under the current EPA security structure, the Office of Environmental Information (OEI) is responsible for:

- Developing and defining the Agency's information security program in accordance with all applicable Federal laws and regulations;
- Providing guidance on selecting and implementing safeguards; and
- Establishing the minimum information security control environment required to protect both its automated data processing resources and its information from theft, damage, and unauthorized use.

EPA regional and program offices are responsible for:

- Establishing an organization-wide information security program consistent with Agency policy, and

- Protecting information and applications by implementing (1) appropriate safeguards into all new organizational information systems, and (2) major modifications to existing systems.

Scope and Methodology

We conducted this audit in accordance with *Government Auditing Standards,* issued by the Comptroller General of the United States. We conducted this audit from January through July 2006 at the National Computer Center in Research Triangle Park, North Carolina, and EPA Headquarters in Washington, DC. We reviewed EPA database security policies and procedures. We tested configuration settings for both the database and operating system software. We interviewed EPA employees and contractors responsible for database maintenance and security.

We selected a judgmental sample of five major financial management database systems that share data with IFMS. We reviewed the following applications during preliminary research:

Application	Acronym	Program Office
Budget Automation System	BAS	Office of the Chief Financial Officer
Financial Data Warehouse	FDW	Office of the Chief Financial Officer
Integrated Resource Management System	IRMS	Office of Research and Development
Office of Pesticide Programs Information Network	OPPIN	Office of Prevention, Pesticides, and Toxic Substances
Strategic Leasing and Asset Tracking Enterprise	SLATE	Office of Administration and Resources Management

We did not review PeoplePlus, EPA's combined human resources and payroll application, because the OIG conducted a security review of the application within the past 12 months.

During preliminary research, we (1) documented management controls surrounding database security, and (2) tested the systems' configuration settings.

- **Management Controls –** We surveyed the respective system owners to determine whether management issued formal policies and procedures for the following key areas: database system configuration, database administrator duties, and system maintenance management. We collected and reviewed the responses, and conducted followup interviews with EPA personnel and contractors. For each system, we reviewed the results of management's latest security control tests.

- **Systems' Configuration Settings –** We conducted vulnerability testing of the selected systems' databases and operating systems to identify common security weaknesses. We used two vulnerability-testing tools recognized by the National Institute for Standards and Technology (NIST). These tools identify potential vulnerabilities and validate that the operating systems and major applications have the latest software versions. We used one tool to test application servers' operating systems for vulnerabilities. We used the other tool to test the database software for vulnerabilities and key database configuration settings. We provided our scanning results to the respective program offices to evaluate the validity of the identified high vulnerabilities. We were unable to conduct vulnerability testing of OPPIN because the program office was relocating the system at the time of our audit. As such, we eliminated OPPIN from our sample.

During field work, we selected three of the five database systems for detailed review. We based our selection on (1) whether an office had documented its database security management control structure, and (2) the total number of "high-risk" vulnerabilities discovered during preliminary testing. We selected BAS, FDW, and IRMS for further review.

We have not performed prior audits related to database security controls for these EPA systems. As such, there were no recommendations to follow up on during this audit.

Chapter 2
Effective Oversight and Continuous Monitoring Needed to Improve Financial Database Security

We discovered weaknesses in how EPA offices (1) monitor financial databases for known security vulnerabilities, (2) share information regarding the implementation of critical system updates, and (3) monitor the use of and access to database administrator accounts and privileges. EPA policies require offices to establish an organization-wide information security program consistent with Agency policy. This includes establishing processes for actively monitoring systems, promptly implementing systems updates, and effectively managing access to network resources and systems. OCFO's policy requires system owners to enter into a Memorandum of Understanding (MOU) when their system interfaces with IFMS. However, this current security oversight process does not incorporate methods that actively monitor the security status of these systems once the MOU is signed. In addition, this policy does not currently apply to systems using means other than an electronic interface to share data with IFMS. As a result, OCFO has limited assurance that the security controls of critical systems adequately protect the accuracy of financial data used for decisionmaking and financial reporting. OCFO needs a more collaborative framework and stronger oversight processes to ensure that systems, which share financial data with IFMS, comply with prescribed Agency security practices.

Consistent Practices Needed to Identify Weaknesses

Offices lack consistent processes to conduct vulnerability testing of systems to identify and correct commonly known security weaknesses. NIST states that it is imperative that organizations routinely test systems for vulnerabilities and misconfigurations to reduce the likelihood of system compromise. EPA policy 2195.1A4, *Agency's Network Security Policy*, requires EPA offices to monitor, test, evaluate, and verify their systems to ensure adequate security in accordance with information sensitivity and other Federal and Agency requirements. Based on interviews with the system owners, we determined that the frequency of vulnerability testing was inconsistent among offices. The vulnerability testing schedules ranged from monthly to only performing the testing in conjunction with completing the major risk assessment, which usually takes place every 3 years. During the time between risk assessments, OCFO does not utilize processes to check the security status of systems that share data with IFMS. As a result, OCFO relies on the implementation of security controls that have become, over time, ineffective due to system changes and emerging system weaknesses.

Our vulnerability test results identified 47 "high-risk," commonly-known security vulnerabilities among the three database systems. Each system had at least 13

"high-risk" vulnerabilities. Some of the identified vulnerabilities had the potential to affect the availability and integrity of the system's financial data. Management could have identified all of the noted vulnerabilities had OCFO's MOU process specified the frequency of vulnerability testing and the offices implemented a routine vulnerability testing process, as required by EPA policy. In addition, NIST Special Publication 800-42, *Guideline on Network Security Testing*, recommends that system owners conduct vulnerability testing at least quarterly to identify and correct vulnerabilities before they are exploited. NIST notes that organizations with an active, priority-driven security-testing program are in a much better position to make prudent investments to enhance the security posture of their systems.

Since IFMS relies heavily on these database systems as the primary source for financial data, vulnerabilities in these systems could allow manipulated data to transfer between systems without notice. Consequently, users of IFMS data could potentially make decisions based on inaccurate data.

We provided the program offices with copies of our vulnerability test results, and the offices indicated they are taking action to remediate the weaknesses. Appendix A contains a high-level summary of the specific technical weaknesses found in each application.

Improvements Needed in Reporting Status of Critical System Patches

OCFO lacks sufficient information to determine whether system owners for systems that share data implement critical system patches. Critical system patches are manufacturer updates to correct significant security vulnerabilities and include other fixes that are prerequisites for the security fixes included in the Critical Patch Update. EPA communicates critical system patches using a high-level alert issued by the Computer Security Incident Response Capability (CSIRC).[1] The CSIRC *Centralized Reporting Guidance* requires the primary Information Security Officer (ISO) for each program and regional office to report status of implementation in accordance with the alert direction. We evaluated whether the applicable program offices adequately reported the implementation status for one high-level alert that affected the three reviewed systems sharing data with IFMS. We found that the primary ISO for the program office responsible for the IRMS system (Office of Research and Development [ORD]) did not report the status for implementing the critical patch to CSIRC or to OCFO. Although ORD officials did not report the patch status to CSIRC, the office indicated that the patch was applied within the specified time period. This occurred, in part, because OCFO management had not implemented processes to (1) inform them when systems that share data requires a critical system patch, and

[1] OEI established CSIRC under the Office of Technology Operations and Planning (OTOP) to serve as the Agency's central system for receiving notifications regarding critical security updates for EPA's information resources. CSIRC is also responsible for notifying system owners when there is a major security update available for their respective applications and tracking the system owners' progress in implementing the system update.

(2) check whether all the systems with which IFMS shares data implemented critical patches. OCFO needs these processes and information to maintain the security and integrity of data shared with IFMS. Without this information, OCFO cannot assess the impact of security threats to IFMS or weaknesses in database systems that could affect the quality of data used for financial management and decisionmaking.

We also determined that the CSIRC could improve its processes for collecting and sharing information regarding the implementation of critical system patches. We reviewed the CSIRC status report regarding each office's implementation of the reviewed high-level alert. We found that 30 percent (7 of 23) of EPA offices provided a complete response to the alert. A complete response indicated that the office took the advised action or the action was not applicable. CSIRC officials indicated that they follow up on incomplete responses with phone calls and emails. However, CSIRC did not document these followup measures in its procedure manual. Nonetheless, at the time of our field work, 4 months had elapsed since the CSIRC issued the alert and many offices had not provided a complete response. In addition, CSIRC does not maintain an inventory of systems in order to determine which offices a particular critical system patch impacts. Also, CSIRC does not share the status report regarding critical system patches with program offices to help them identify and mitigate unresolved security vulnerabilities in systems with which they share data. Sharing the status of implemented critical system patches would (1) provide ISOs with a tool to more proactively manage the security of their database systems, and (2) allow the CSIRC to focus its limited resources on analyzing emerging security threats. Because of these weaknesses, EPA's CSIRC lacks the capability to assess the potential impact that unimplemented critical patches have on the Agency's network resources.

Database Administrator Accounts and Privileges Not Managed Properly

System owners do not adequately control users' access to and use of database administrator accounts and privileges, as required by EPA policy 2195.1A4, *Agency's Network Security Policy***.** In particular, the policy requires passwords and user login IDs to be unique and not shared. The policy also requires system authorizations to be restricted to the minimum level of access necessary for a person to do their job. Our testing found instances where:

- Multiple people were sharing database administrator account user login IDs and passwords. The database administrator account privileges provide complete and unrestricted access to all data in the database. When user login IDs and passwords are shared, EPA loses the ability to hold users accountable for their actions within the system.

- Users could excessively access sensitive database components or execute high-level commands. A database component or "object" could be the database table or information stored in the database table. A high-level command or "privilege" allows the user to create or manipulate objects, such as data tables and/or reassign system privileges to other personnel without authorization.

Properly controlling/administering these features is important because they allow management to (1) hold users that make inappropriate system changes accountable, (2) limit system privileges of each user to only those the user needs to perform their job, and (3) control unauthorized reassignment of system privileges to other personnel.

These weaknesses exist, in part, because the OCFO's MOU process does not specify the standards for monitoring the access and use of high-level database accounts. In addition, the system owners did not implement effective management control processes to ensure that security personnel comply with EPA security policy. Furthermore, management had not implemented processes to review access to and use of database administrator accounts and privileges. As a result, offices granted many of the database security privileges in a way that allowed users to re-assign their system access to other users without the knowledge of the office. We provided the respective program offices with copies of our test results, and the offices indicated that they are taking action to remediate the weaknesses. Appendix A contains a high-level summary of the specific technical weaknesses found in each application.

Recommendations

We recommend that the Office of the Chief Financial Officer, Information Security Officer:

1. Update the MOU process to include formal security Standards that require program and regional offices to actively monitor the security status of systems that share data with IFMS. These standards should require all system owners to:

   a. Perform network vulnerability testing at least quarterly in accordance with NIST 800-42, *Guideline on Network Security Testing*, and remediate identified vulnerabilities in a timely manner.

   b. Monitor the use of and access to high-level system functions (such as Accountability, Least Privilege, Separation of Duties, etc.) at least monthly to ensure adequate controls are applied and effective.

c. Certify that the program/regional office has put in place oversight processes to ensure these information security standards are met.

2. Request from OEI access to information regarding the implementation status of high-risk CSIRC critical system patches for systems that share data with IFMS.

3. Develop and implement formal procedures to ensure all OCFO system owners timely and accurately report progress for implementing Computer Security Incident Response Capability critical system patches.

We recommend the Director of Office of Technology Operations and Planning within the Office of Environmental Information:

4. Strengthen, formalize, and evaluate the effectiveness of the followup procedures for obtaining complete responses from program and regional offices regarding high-level critical system patch alerts.

5. Develop and implement a formal process to share EPA-wide status reports with ISOs regarding implementation of CSIRC critical system patches.

We recommend the system owners for the (1) Budget Automated System (OCFO System), (2) Financial Data Warehouse (OCFO System), and (3) Integrated Resources Management System (ORD System):

6. Correct all identified system weaknesses disclosed in Appendix A.

7. Develop a Plan of Action and Milestones in the Agency's security weakness tracking system (ASSERT database) for all uncorrected deficiencies disclosed in Appendix A.

Agency Response and OIG Comments

ORD concurred with the report findings and recommendations. However, OCFO officials did not agree with the report recommendations, citing that its current MOU process provided the appropriate level of oversight. OEI officials also did not agree with the report's recommendations. OEI indicated the office has a process in place for tracking responses to high-level critical system patch alerts. In addition, OEI indicated that the office's current status report provided to management and ISOs for the purpose of their distributed oversight is sufficient.

We met with Agency officials from all three offices subsequent to receiving their responses to the draft report. Based on our discussions, OCFO and OEI officials agreed that the offices could take more steps to improve the current processes and

strengthen database security. As such, OCFO agreed to modify its MOU process to provide more specificity to system owners with systems that share data with IFMS. OCFO also agreed to take steps to ensure all OCFO system owners timely and accurately report progress for implementing critical system patches. OEI officials agreed to formalize their CSIRC followup procedures and make critical patch reports more available. Where appropriate, we modified the report to address the offices' concerns and our discussions.

OEI and ORD provided a corrective action plan to address the report's findings and recommendations. OCFO updated its response to the report and indicated that the office would provide a corrective action plan to address the remaining open recommendations. Complete responses are provided in Appendices B, C, and D.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in $000s)	
Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Claimed Amount	Agreed To Amount
1	7	Update the MOU process to include formal security Standards that require program and regional offices to actively monitor the security status of systems that share data with IFMS. These standards should require all system owners to: a. Perform network vulnerability testing at least quarterly in accordance with NIST 800-42, *Guideline on Network Security Testing*, and remediate identified vulnerabilities in a timely manner. b. Monitor the use of and access to high-level system functions (such as Accountability, Least Privilege, Separation of Duties, etc.) at least monthly to ensure adequate controls are applied and effective. c. Certify that the program/regional office has put in place oversight processes to ensure these information security standards are met.	O	Information Security Officer, Office of the Chief Financial Officer			
2	8	Request from OEI access to information regarding the implementation status of high-risk CSIRC critical system patches for systems that share data with IFMS.	O	Information Security Officer, Office of the Chief Financial Officer			
3	8	Develop and implement procedures to ensure all OCFO system ownes timely and accurately report progress for implementing CSIRC critical system patches.	O	Information Security Officer, Office of the Chief Financial Officer			
4	8	Strengthen, formalize, and evaluate the effectiveness of the followup procedures for obtaining complete responses from program and regional offices regarding high-level critical system patch alerts.	C	Director, Office of Technology Operations and Planning	08/01/2007		
5	8	Develop and implement a process to share EPA-wide status reports with Information Security Officers regarding implementation of CSIRC critical system patches.	C	Director, Office of Technology Operations and Planning	08/01/2007		
6	8	Correct all identified system weaknesses disclosed in Appendix A.	C	BAS System Owner FDW System Owner IRMS System Owner	BAS-05/2006 FDW-08/2006 IRMS-04/ 2006		
7	8	Develop a Plan of Action and Milestones in the Agency's security weakness tracking system (ASSERT database) for all uncorrected deficiencies disclosed in Appendix A.	C	BAS System Owner FDW System Owner IRMS System Owner	BAS – N/A FDW – N/A IRMS – N/A		

[1] O = recommendation is open with agreed-to corrective actions pending
C = recommendation is closed with all agreed-to actions completed
U = recommendation is undecided with resolution efforts in progress

Appendix A

High-Level Summary of Specific Technical Weaknesses by EPA Program Office and System[2]

This Appendix is for restricted distribution. This Appendix contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of these findings, the Office of Inspector General removed this Appendix from the public version of the report.

[2] A detailed listing of technical weaknesses was provided to the respective Program Office officials. The detailed listing identified the specific weaknesses, to include background information on the weaknesses and possible methods the system owner could use to correct the weaknesses.

Appendix B

Non-Sensitive Portion of OCFO's and OEI's Combined Response to Draft Audit Report

February 23, 2007

MEMORANDUM

SUBJECT: Office of the Chief Financial Officer (OCFO) Response to the Office of Inspector General's (OIG) Draft Audit Report – EPA Needs to Strengthen Financial Database Security Oversight and Monitor Compliance, Dated January 11, 2007, Assignment No. 2006-000442

FROM: Krista Mainess, Director
Office of Program Management
Office of the Chief Financial Officer

TO: Rudy Brevard
Acting Director, Business Systems Audits

We appreciate the opportunity to provide written comments on the subject draft audit report. The OCFO remains firmly committed to securing its systems and data in a cost effective manner and in accordance with Federal guidance, EPA policy, and best practices.

If you or your staff have any questions or need additional information concerning our response to the subject draft report, contact Bob Shields, IT Team Leader, at 202-564-0123.

cc: Lyons Gray, OCFO
Maryann Froehlich, OCFO
Lorna McAllister, OCFO
David Bloom, OCFO
Mitch Gray, OCFO
Myra Galbreath, OEI
Marian Cody, OEI
Pat Hill, OIG

Below you will find general comments on the entire report as well as specific comments related to each recommendation.

OCFO's General Comment:
Much of the audit text appears to be based on the assumption that IFMS "shares data" with FDW, BAS, and IRMS, but the report provides no details on what this means.

Here are details on each system's relationship to IFMS. The FDW copies data from IFMS for reporting. IFMS receives no data from the FDW. BAS has no connection to send or receive data with IFMS. IRMS transmits commitment and reprogramming documents to IFMS. Those documents are subject to all IFMS edits before they are processed so there are already safeguards built into the process.

Transactions entered in IFMS are monitored by a particular user community. For example, if IRMS transmitted invalid commitments to IFMS that still passed the accounting string and funds availability edits, they would be discovered by ORD (the owner of IRMS) and corrected. The OCFO, Office of Budget in their annual closeout memo requires allowance holders to monitor their available funds. They issued their 2007 closeout memo on December 18, 2006.

Another example of a transaction control on IFMS data is the annual year-end certification of unliquidated obligations. Allowance holders are required to certify to OFM that their unliquidated obligation balances in IFMS are correct. This requirement is documented in the annual financial statement audit commitment memorandum signed by the Chief Financial Officer and the Inspector General. Details on the process are included in the OFM year end closing memo.

Finally, many of the recommendations directed toward the OCFO ISO are the responsibility of the individual system owners, according to EPA's Information Security Manual 2195A.

OARM's General Comment:
SLATE does not receive nor send data to IFMS.

OEI's General Comment:
The procedures requested for developing and implementing recommendation #3 were in place prior to this audit finding and have been previously provided.

In addition, the following inaccuracies in the draft audit are noted. One area of concern is the apparent confusion regarding CSIRC's roles and responsibilities. CSIRC maintains an inventory of the Agency's technologies so that they can notify the Information Security Officers to upgrade or patch their systems. CSIRC is not responsible for determining which informational systems are critical to the Agency. However, CSIRC does determine which patch is critical.

OIG recommendations and corresponding OCFO/OEI responses are as follows:

OIG Recommendation #1:
The Information Security Officer (ISO) within the Office of the Chief Financial Officer (OCFO) update the Memorandum of Agreement process to include formal security standards that require the program/regional offices to actively monitor the security status of systems that share data with IFMS. These standards should require all system owners to:

a. Perform network vulnerability testing at least quarterly in accordance with NIST 800-42, Guideline on Network Security Testing, and remediate identified vulnerabilities in a timely manner.

b. Monitor the use of and access to high-level system functions (such as Accountability, Least Privilege, Separation of Duties, etc.) at least monthly to ensure adequate controls are applied and effective.

c. Certify that the program/regional office has put in place oversight processes to ensure these information security standards are met.

CFO Response to Recommendation #1:
The OCFO agrees with this recommendation.

OIG Recommendation #2:
The ISO within OCFO request from OEI access to information regarding the implementation status of high risk CSIRC critical system patches for systems that share data with IFMS.

OCFO Response to Recommendation #2:
The OCFO agrees with this recommendation.

OIG Recommendation #3:
The ISO within OCFO send out a notification to all OCFO system owners reminding them of the criticality of timely and accurately reporting the status of implementing CSIRC critical system patches.

OCFO Response to Recommendation #3:
The OCFO agrees with this recommendation.

OEI Recommendation #4:
Develop and implement follow-up procedures to obtain complete responses from program and regional offices regarding high-level critical system patch alerts.

OEI Response to Recommendation #4:
OEI does not concur with this recommendation.

OEI/OTOP has a process in place for tracking responses to high-level critical system patch alerts, which includes following up with Information Security Officers (ISOs). If the system is a Microsoft based platform, CSIRC uses PatchLink for progress reports and contacts ISOs regarding any delay in patch implementation. In addition, CSIRC acts as a liaison between Network Infrastructure Services (NIS http://lansys.epa.gov/)ISOs and PatchLink Administrators regarding any problems with patch deployment. If the system is not a Microsoft based platform, the ISOs are responsible for reporting the patch status to CSIRC. CSIRC follows up according to the time constraints provided in the CSIRC-Alert. For a critical or high-level patch, response is required within two business days. If a response is not received, CSIRC contacts all ISOs with applicable systems in their area for patch status information. It should be noted that the responsibility for the patching of systems does not fall under CSIRC. It is the responsibility of each region and program office to act on CSIRC-Alerts and patch their systems accordingly.

In addition, CSIRC has provided information to NCC Security regarding the potential impact that unimplemented critical patches have on the Agency's network resources in emails, Security Incident Request (SIR) tickets, and Quarterly Reports. CSIRC does not implement or govern patch deployment, nor does it have the authorization to enforce.

OIG Recommendation #5:
Develop and implement a process to share EPA-wide status reports with Information Security Officers regarding implementation of CSIRC critical system patches.

OEI Response to Recommendation #5:
OEI does not concur with this recommendation.

Traditionally, the Agency has maintained that the specific vulnerabilities and security postures of the regions and program offices will not be shared EPA-wide. However, we currently provide reporting status to management and ISOs for the purpose of their distributed oversight. OTOP will continually work to create a more streamlined reporting process.

Appendix C

OCFO's Response to Recommendations Associated with Sensitive Technical Control Weaknesses Disclosed in Appendix A

This Appendix is for restricted distribution. This Appendix contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of these findings, the Office of Inspector General removed this Appendix from the public version of the report.

Appendix D

ORD's Response to Recommendations Associated with Sensitive Technical Control Weaknesses Disclosed in Appendix A

This Appendix is for restricted distribution. This Appendix contains material that is confidential business information, proprietary information, or source selection information. Unauthorized disclosure of this Appendix or any of its content may violate the provisions of the Trade Secrets Act, 18 U.S.C. 1905; the Procurement Integrity Act, 41 U.S.C. 423; the Freedom of Information Act, 5 U.S.C. 552; the Privacy Act, 5 U.S.C. 552a; and/or the Federal Acquisition Regulation, Section 3.104 (48 CFR 3.104). Due to the sensitive nature of these findings, the Office of Inspector General removed this Appendix from the public version of the report.

Appendix E

Distribution

Office of the Administrator
Chief Financial Officer (CFO)
Assistant Administrator for Environmental Information
Assistant Administrator for Research and Development
Agency Followup Coordinator
Audit Followup Coordinator, Office of the Chief Financial Officer
Audit Followup Coordinator, Office of Environmental Information
Audit Followup Coordinator, Office of Research and Development
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Office of General Counsel
Acting Inspector General