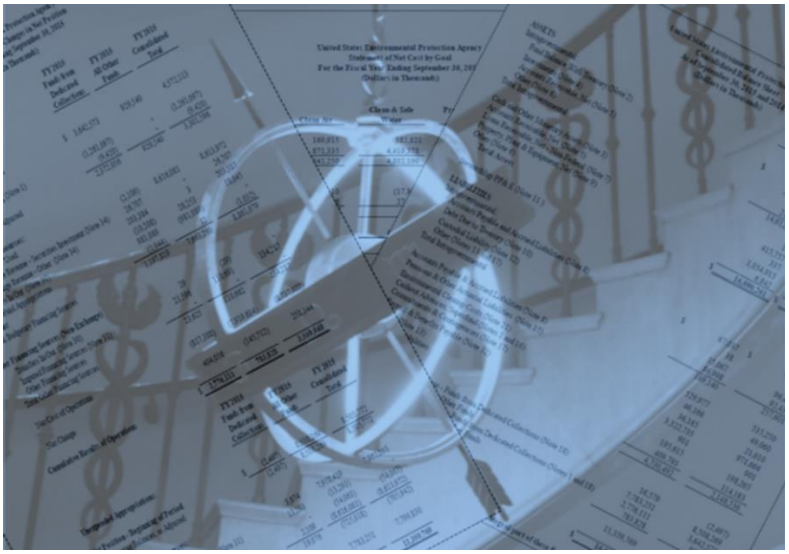
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Information Technology

Controls Needed to Track Changes to EPA's Compass Financials Data

Report No. 17-P-0205 **May 8, 2017**



Report Contributors:

Rudolph M. Brevard
Albert E. Schmidt
Jeremy Sigel
Sabrena Stewart

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FRB	Function Review Board
FY	Fiscal Year
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OTS	Office of Technology Solutions
SOPs	Standard Operating Procedures
SP	Special Publication

Cover image: EPA OIG-generated graphic.

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

17-P-0205
May 8, 2017

At a Glance

Why We Did This Review

We conducted this audit to determine whether the U.S. Environmental Protection Agency's (EPA's) Office of the Chief Financial Officer (OCFO) has implemented controls to prevent and detect unauthorized changes made directly to the EPA's financial data in Compass Financials.

Because Compass Financials is a commercial off-the-shelf software program, there are certain parameters and settings that EPA system administrators must use to tailor the functionality of the web-based application to meet the agency's needs. The EPA must also use controls to enforce security over the tailored configuration changes, as well as any changes made to data via direct modifications performed by individuals with access to the Compass Financials database.

This report addresses the following EPA goal or cross-agency strategy:

- *Protecting human health and the environment by enforcing laws and assuring compliance.*

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

Controls Needed to Track Changes to EPA's Compass Financials Data

What We Found

OCFO needed to strengthen internal controls in order to certify that any changes made to the Compass Financials application are implemented based on management approval. Specifically, OCFO lacked documentation that supports the approval and verification of direct modifications made to the Compass database. OCFO also lacked procedures for handling emergency or unscheduled configuration changes made to OCFO financial information systems.

Without the review, approval and verification of direct modifications and configuration changes to Compass Financials by the Functional Review Board, personnel with access to the system could modify key EPA financial data. OCFO updated its procedures and took sufficient actions to address our recommendations.

Federal and agency guidance require the agency to do the following:

- Establish and follow a process to protect applications and data from unauthorized access and modification.
- Document procedures for the handling of emergency or unscheduled changes.

Occasionally, modifications need to be made to data within the Compass database, and the changes cannot be performed through the users' web interface. We tested 10 direct modifications to Compass Financials data to determine whether the modifications were authorized for implementation, and whether the changes were implemented as intended. We found the approvals and verifications of completion were not documented as required. There was no assurance that changes were implemented as intended. Further, unauthorized changes to the data could go undetected.

Unauthorized changes may have hampered the ability of EPA program managers and other decision-makers to use Compass Financials information to track, evaluate and analyze the cost of operations in accomplishing program initiatives and activities designed to protect human health and the environment.

Recommendations and Agency Corrective Actions Taken

The EPA took corrective actions to complete the three recommendations within the report. The corrective actions taken by the agency address the intent of our recommendations and corrected the identified deficiencies. We consider all three recommendations closed with corrective actions completed.

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

THE INSPECTOR GENERAL

May 8, 2017

MEMORANDUM

SUBJECT: Controls Needed to Track Changes to EPA's Compass Financials Data
Report No. 17-P-0205

FROM: Arthur A. Elkins Jr.

TO: David Bloom, Acting Chief Financial Officer
Office of the Chief Financial Officer

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY16-0056. 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.

Action Required

You are not required to provide a written response to this final report because you took corrective actions to complete the three report recommendations. We consider all recommendations resolved and closed. Should you choose to provide a final response, we will post your response on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Appendices

Purpose

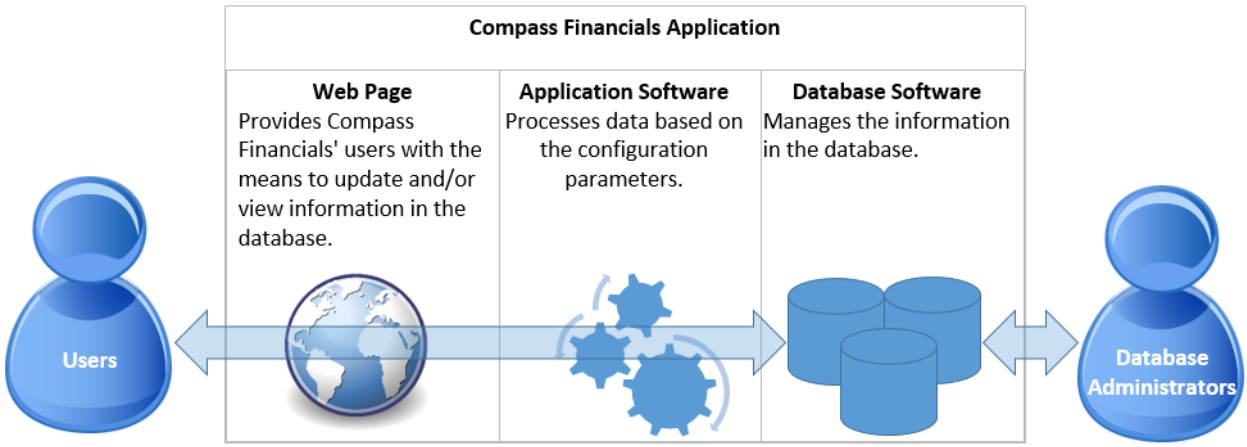
The Office of Inspector General (OIG) for the U.S. Environmental Protection Agency (EPA) conducted this audit to determine whether the EPA's Office of the Chief Financial Officer (OCFO) has implemented controls to prevent and detect unauthorized changes made directly to the EPA's financial data in Compass Financials.

Background

Compass Financials is a web-based application developed, hosted, operated and maintained by a service provider. Users of Compass Financials software use the Compass Financial web page to process financial transactions. Periodically, corrections or modifications need to be made to information within the Compass Financials database, and the modifications cannot be performed through the users' input screens. In addition, configuration changes need to be made to the Compass application. These changes could include unscheduled or emergency changes. Figure 1 provides an overview of Compass Financials.

Compass Financials is the EPA's primary financial application. During fiscal year (FY) 2016, the EPA's budget of $8.1 billion would have been processed through Compass Financials.

Figure 1: Overview of Compass Financials



Source: EPA OIG analysis.

Note: Most users enter Compass Financials through the application's web page. Through the web page, the user can access or view Compass information stored in the Compass database. Database administrators configure and manage the security and functionality of the Compass database. The database administrators can also bypass the application's security and functionality, and directly access information in the database.

EPA program managers and other decision-makers use the information in Compass Financials to track, evaluate and analyze the cost of accomplishing program initiatives and activities designed to protect human health and the environment.

Because Compass Financials is a commercial off-the-shelf software program, there are certain parameters and settings that EPA system administrators must use to tailor the functionality of the web-based application to meet the agency's needs. The EPA must also use controls to enforce security over the tailored configuration changes, as well as any changes made to data via direct modifications performed by individuals with access to the Compass database.

The National Institute of Standards and Technology (NIST) provides guidance in its NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, April 2013. NIST SP 800-53 provides guidance for monitoring and tracking administrator access and configuration management used to modify applications and data. This guidance helps to prevent unauthorized changes to the application and the data contained within the application.

Responsible Offices

The OCFO is responsible for direct modifications to data and system configuration changes for all OCFO systems, including Compass Financials. Within OCFO, the Office of Technology Solutions (OTS) developed the *Change Control Process for Service Requests Standard Operating Procedures* (SOPs). The SOPs define the process for data modifications and system configuration changes for OCFO systems managed by OTS, including Compass. In addition, OTS is also responsible for tracking the requests for data modifications and system configuration changes.

OTS developed a change control process for changes to application software, and operational support requests including data fixes. These processes cover all OTS systems, including Compass.

Scope and Methodology

We performed this audit from November 2015 through February 2017. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report pertains to the EPA's compliance with applicable laws, regulations and agency guidance. We evaluated the process used by the EPA to directly

modify the Compass Financials data and configuration. We interviewed OCFO personnel in Washington, D.C. We tested a judgmentally selected sample of 10 out of 43 known direct modifications of the Compass Financials database, which occurred between April and October 2015. These changes include updates to the vendor table, vendor payee records and other changes that occurred during this period. Appendix A contains a list of the 10 changes tested.

Prior Reporting

In EPA OIG Report No. 17-F-0046, *EPA's Fiscal Years 2016 and 2015 Consolidated Financial Statements*, issued November 15, 2016, we reported that the EPA did not establish controls to prevent or detect unauthorized access to the Compass Financials database. A breach of information in the Compass Financials database, which houses Personally Identifiable Information belonging to employees and vendors, could cost the EPA as much as $3.5 million, including the costs to detect, recover, investigate and manage the incident response. A breach also could include costs that result in after-the-fact activities and efforts to contain additional costs.

We recommended that the EPA work with the Compass Financials service provider to establish controls for creating and locking administrative accounts, and to implement a methodology to monitor accounts with administrative capabilities. We also recommended that the EPA record this weakness in the agency's system used for monitoring the remediation of information security corrective actions. The agency indicated that they would be completing the corrective actions for these two recommendations by the end of the 4th quarter of FY 2021.

Results of Review

Direct modifications to the Compass Financials database lacked documented approvals, and the verifications of implemented changes to the Compass database as required by federal and agency guidance. In addition, OCFO did not have a documented process for handling emergency or unscheduled changes to the OCFO financial system's configuration.

Agency guidance requires OCFO personnel to follow change control procedures in OCFO's SOPs to ensure the integrity, security and reliability of EPA systems and data. OCFO representatives indicated that the procedures for approvals and verifications of direct modifications to the Compass database documented in the SOPs did not reflect the current process. Further, OCFO representatives indicated that their change procedures were outdated. As a result, unauthorized and unverified modifications of Compass data and configuration could occur.

Direct Modifications to Compass Financials Database Lacked Documented Approvals and Verifications

Compass Financials configuration changes, performed via direct modification, lacked documented approvals and verifications that the change was implemented as intended. The descriptions for the 10 tested direct database modifications to the Compass Financials database included changes to vendor information, and an update to payment subsidy tables.

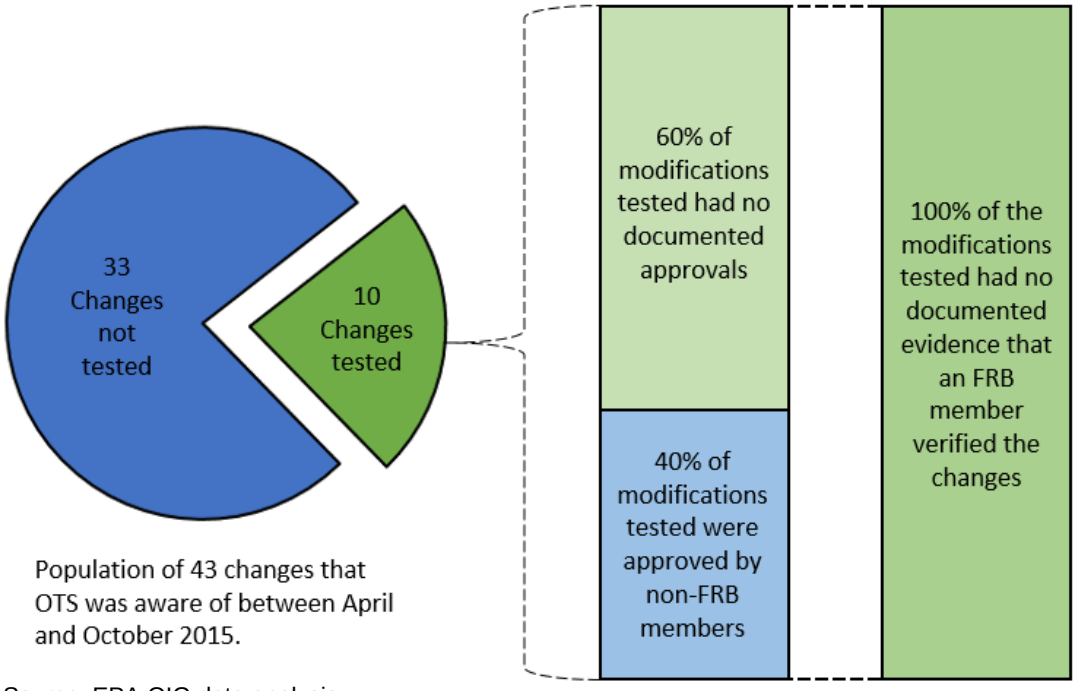
Figure 2 illustrates the 10 sampled changes that include the following:

The Functional Review Board is responsible for reviewing and prioritizing change requests for OTS systems.

- A Functional Review Board (FRB) member did not approve implemented changes for any of the 10 sampled changes as required by the SOPs.
    - Four modifications were approved by individuals who were not FRB members.
    - There was no documentation to substantiate that the other 6 out of 10 sampled changes were approved by an FRB member.

- The OTS was unable to provide FRB verification of change work performed for any of the 10 sampled changes, as required by the FRB.

Figure 2: EPA compliance with required change controls for Compass Financials data change requests



Source: EPA OIG data analysis.

The Federal Information Security Modernization Act tasked the NIST with the responsibility of developing minimum information security requirements, as provided in NIST SP 800-53. Security control number CM [Configuration Management] -3, *Configuration Change Control*, within NIST SP 800-53, requires an organization to review proposed configuration-controlled changes and only implement approved changes.

The EPA's Configuration Management Policy, as provided through the Chief Information Officer or CIO 2123.1, states the following:

> EPA Program Offices and Regions must meet or exceed all Federal regulatory policies and procedures which affect Configuration and Change Management processes to be implemented on EPA information technology assets.

The Compass Financials service provider's technical team executes changes via Structure Query Language updates directly to Compass Financials data. The SOPs require these direct modifications to receive the following approval and verification:

Structure Query Language is a computer programming language designed for managing data held in database management systems.

- FRB approval prior to implementation.
- FRB verification that the change was successfully implemented.

The required approval and verification were not documented, because OTS personnel managing the change control process for Compass Financials followed a process for tracking data fixes that did not comply with the guidelines in the SOPs. Without documented approval and verification, there is no evidence that changes were approved or verified. As a result, there was no documented support that OTS personnel obtained FRB approval prior to implementing the data fixes. In addition, there was no documented support that FRB members verified whether the data changes were successfully implemented.

Without the review, approval and verification of change requests for direct modification to Compass Financials, personnel with access to the system could modify key financial data without accountability. This lack of oversight put the integrity of Compass Financials data at risk and compromise the integrity of EPA financial information used by decision-makers to protect human health and the environment.

OCFO Lacked Emergency or Unscheduled Change Procedures for Its Information Systems

OCFO lacked procedures for handling emergency or unscheduled changes of its financial systems. NIST SP 800-128, dated August 2011, *Guide for Security-*

Focused Configuration Management of Information Systems, Section 3.2.2, *Implement the Configuration Change Control Process*, requires that an organization do the following:

> [I]nclude instructions for handling [emergency] unscheduled changes within the configuration change control procedures as well as instructions for handling unauthorized changes that are subsequently discovered.

The EPA's Configuration Management Policy, CIO 2123.1, states the following:

> Each Program Office and Region must document, implement, and maintain Configuration and Change Management processes, in collaboration with the Office of Environmental Information, Office of Technology Operations and Planning.

OTS did not develop procedures for handling emergency or unscheduled changes. In February 2013, OTS issued the *Change Control Process for Service Requests Standard Operating Procedures.* However, the procedure document did not provide guidance for handling emergency change requests. OTS personnel indicated that they issued the SOPs during the early stages of the Compass Financials system development. OTS personnel stated that this document was not fully developed and became outdated as the Compass Financials processes underwent changes.

Without documented emergency change procedures for OCFO systems, such as Compass Financials, changes could be implemented without required authorization or approvals. As such, the lack of controls over unscheduled modifications to Compass Financials configuration and databases could compromise the security of EPA financial resources that agency officials use for making decisions to protect human health and the environment.

Conclusion

In order to maintain system integrity, it is essential to have control over modifications of OCFO systems, as well as have control of the configuration management process. The EPA faced the potential that unauthorized modifications may be made to OCFO systems and data. This could have resulted in the EPA being unable to effectively track, evaluate and analyze the cost of operations in accomplishing program initiatives and activities designed to protect human health and the environment.

Recommendations

We recommended that the Chief Financial Officer:

1. Require personnel responsible for controlling changes to Compass Financials to follow established standard operating procedures for approvals from authorized Functional Review Board members prior to implementation, and have a board member verify the changes were implemented correctly.

2. Establish procedures for handling unscheduled or emergency changes for Office of the Chief Financial Officer financial systems.

3. Provide training to personnel responsible for controlling changes to Compass Financials and require them to follow established standard operating procedures. This includes training personnel on newly developed procedures for handling unscheduled or emergency changes.

Agency's Response and OIG Evaluation

Subsequent to issuing our draft report in February 2017, the agency provided supporting documentation that showed it has completed all recommended corrective actions. As such, the EPA indicated it disagreed with all three recommendations.

However, the corrective actions taken by the EPA correct the identified deficiencies and fully address our concerns. We consider all three recommendations to be resolved and closed with corrective actions completed.

The agency's full written response and OIG comments are found in Appendix B.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Completion Date	Potential Monetary Benefits (in $000s)
1	7	Require personnel responsible for controlling changes to Compass Financials to follow established standard operating procedures for approvals from authorized Functional Review Board members prior to implementation, and have a board member verify the changes were implemented correctly.	C	Chief Financial Officer	3/8/17	
2	7	Establish procedures for handling unscheduled or emergency changes for Office of the Chief Financial Officer financial systems.	C	Chief Financial Officer	3/28/17	
3	7	Provide training to personnel responsible for controlling changes to Compass Financials and require them to follow established standard operating procedures. This includes training personnel on newly developed procedures for handling unscheduled or emergency changes.	C	Chief Financial Officer	3/29/17	

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

Listing of Data Modifications Tested

Sample #	Agency tracking #	Description of the change
1	14335	Update to vendor table.
2	14566	Update to reference table.
3	14630	Update to Payment Subsidy tables.
4	16155	Update to Obligation Header.
5	16304	Update to vendor data.
6	16892	Update to vendor data.
7	24182	Remove orphaned vendor record.
8	16645	Linked vendor name change.
9	16963	Issues with SV.
10	16983	Run several Sequels for WCF.

Appendix B

Agency's Full Response and OIG Comments

APR 04 2017

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Audit Project No. OA-FY16-0056, "*Controls Needed to Track Changes to EPA's Compass Financials Data,"* dated February 27, 2017

FROM: David A. Bloom, Acting Chief Financial Officer
Office of the Chief Financial Officer

TO: Rudy M. Brevard, Director
Information Resources Management Audits

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. The following is a summary of the agency's overall position along with its position on each of the report recommendations.

AGENCY'S OVERALL POSITION

The agency does not agree with all three of the recommendations in the draft report. Based on additional information provided and subsequent conversations, we request that the final report be closed upon issuance.

AGENCY'S RESPONSE TO DRAFT AUDIT RECOMMENDATIONS

Disagreements

No.	Recommendation	Agency Explanation/Response	Proposed Alternative
1	We recommend that the Chief Financial Officer require personnel responsible for controlling changes to Compass Financials to follow established standard operating procedures for approvals from authorized Functional Review Board members prior to	The OCFO updated the Configuration Management Standard Operating Procedures and provided the SOPs to personnel responsible for controlling changes to Compass Financials. The documents were provided to the Office of the Inspector General in March 2017.	N/A

	implementation, and have a Functional Review Board member verify the changes were implemented correctly.		

OIG Response 1: On March 8, 2017, the OCFO provided documentation that supports it currently following established standard operating procedures, and obtaining approvals from authorized Functional Review Board members prior to implementing system changes. The OCFO is also having a Functional Review Board member verify the changes were implemented correctly. As such, the OCFO took sufficient action to address our recommendation.

2	We recommend that the Chief Financial Officer establish procedures for handling unscheduled or emergency changes for Office of the Chief Financial Officer financial systems.	The OCFO developed a Change Management Charter and updated the Configuration Management SOPs and Functional Review Board Procedures for handling unscheduled or emergency changes. The documents were provided to the OIG in March 2017.	N/A

OIG Response 2: Subsequent to the issuance of our draft report in February 2017, the OCFO approved a Change Management Charter, and updated the Configuration Management SOPs and the Functional Review Board Procedures. The OCFO approved the related documents on March 29, 2017. As a result, the OCFO took sufficient action to address our recommendation.

3	We recommend that the Chief Financial Officer provide training to personnel responsible for controlling changes to Compass Financials and require them to follow established standard operating procedures. This includes training personnel on the newly developed procedures for handling unscheduled or emergency changes.	The OCFO developed a Change Management Charter and updated the Configuration Management SOPs and FRB Procedures for handling unscheduled or emergency changes. The documents were provided to the OIG in March 2017. The OCFO provided training to personnel responsible for controlling changes to Compass Financials at a variety of meetings over the past several months.	N/A

OIG Response 3: The OCFO approved a Change Management Charter, and updated the Configuration Management SOPs and the Functional Review Board Procedures to include procedures for handling unscheduled or emergency changes. The OCFO did not provide documentation that supports the office personnel trained on these procedures. However, the OCFO provided evidence that the procedures are being followed, and this demonstrates a higher level of compliance with established procedures now than what was present during our audit fieldwork. As such, these actions address our concern and we consider the recommendation completed.

CONTACT INFORMATION

If you have any questions regarding this response, please contact the OCFO's Audit Follow-up Coordinator, Benita Deane, at 202-564-2292.

cc: Charles Sheehan
Kevin Christensen
Richard Eyermann
Howard Osborne
Quentin Jones
Robert Hill
Lisa Ayala
Alexandra Sullivan
Jeanne Conklin
Meshell Jones-Peeler
Sherri Anthony
Rudy Brevard
Bob Trent
Benita Deane
Susan Lindenblad

Appendix C

Distribution

The Administrator
Chief of Staff
Chief Financial Officer
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Associate Chief Financial Officer
Controller, Office of the Controller, Office of the Chief Financial Officer
Deputy Controller, Office of the Controller, Office of the Chief Financial Officer
Director, Office of Budget, Office of the Chief Financial Officer
Director, Office of Planning, Analysis and Accountability, Office of the Chief Financial Officer
Director, Office of Technology Solutions, Office of the Chief Financial Officer
Director, Office of Resource and Information Management, Office of the Chief Financial Officer
Director, Office of Information Security and Privacy, Office of Environmental Information
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of the Chief Financial Officer