U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S Consolidated Business Information System FY 2011

Report No. **4A-CF-00-11-015**

Date: June 1, 2011

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S CONSOLIDATED BUSINESS INFORMATION SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CF-00-11-015

Date: 06/01/11

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S CONSOLIDATED BUSINESS INFORMATION SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CF-00-11-015

Date: 06/01/11

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Consolidated Business Information System (CBIS). Our conclusions are detailed in the "Results" section of this report.

The Office of the Inspector General (OIG) reviewed the CBIS security program and found that the following areas appeared to be in full FISMA compliance:

- A security certification and accreditation (C&A) of CBIS was completed in September 2009.
- The OIG agrees with the security categorization of moderate for CBIS.
- The Information System Security Plan for CBIS contains the critical elements required by National Institute of Standard and Technology (NIST) Special Publication (SP) 800-18.
- A risk assessment was conducted for CBIS in September 2009 that addresses all the required elements outlined in relevant NIST guidance.
- An independent security test and evaluation (ST&E) was completed for CBIS as a part of the system's C&A process in September 2009.

- The designated security officer for CBIS conducted a self-assessment of the system in September 2010.
- A contingency plan was developed and tested for CBIS in March 2010 in compliance with NIST SP 800-34.

However, we noted the following opportunities for improvement in the CBIS security program:

- The CBIS Privacy Impact Assessment (PIA) was not conducted in full compliance with the requirements of OPM's PIA Guide and the Office of Management and Budget (OMB) Memorandum M-03-22.
- The CBIS POA&M does not contain all known security weaknesses as required by the OPM POA&M Guide.
- The OIG independently tested 28 of the NIST 800-53 controls for CBIS and found that 7 of these security controls were not in place during the fieldwork phase of the audit.

In addition to the weaknesses outlined above, we noted a significant deficiency in the Office of the Chief Financial Officer's (OCFO) ability to manage segregation of duties within the CBIS application. The OCFO developed a segregation of duties policy, but the application did not have the technical settings in place to enforce these rules. In addition, the OCFO indicated that they did not have a firm understanding of the roles that should be segregated within the application and that the existing segregation of duties policy was not accurate.

Contents

Page

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Consolidated Business Information System (CBIS).

Background

CBIS is one of OPM's 43 critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

The Office of the Chief Financial Officer (OCFO) has been designated with ownership of CBIS. CBIS aids in OPM's management of the agency's financial resources. CBIS provides functionality for OPM's general ledger, accounts payable, accounts receivable, purchasing, procurement, budgeting, and other financial resources management. OPM's Center for Financial Services within the OCFO is responsible for the CBIS system. The OPM OCFO has retained Accenture to implement, host, and operate CBIS.

In 2009, the OIG conducted an audit of the system development and implementation of CBIS. As part of this current audit, we followed up on prior audit recommendations related to CBIS IT security. One audit recommendation from the 2009 report is reissued in this report (see Recommendation 1).

We discussed the results of our audit with OCFO representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of security controls for CBIS to ensure that OCFO officials have implemented IT security policies and procedures in accordance with standards established by OPM, FISMA, and the National Institute of Standards and Technology (NIST).

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The overall audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for CBIS, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;

- Independent Security Control Testing;
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of OCFO officials responsible for CBIS, including IT security controls in place as of January 2011.

We considered the CBIS internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objective, we interviewed representatives of OPM's OCFO office and Accenture officials with CBIS security responsibilities. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of CBIS are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on CBIS's system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;

- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November 2010 through January 2011 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OCFO's management of CBIS is consistent with applicable standards. Nothing came to the OIG's attention during this review to indicate that the OCFO is in violation of relevant laws and regulations.

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of CBIS was completed in September 2009.

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. The CBIS C&A appears to have been conducted in compliance with NIST guidance.

The U.S. Department of Transportation's Enterprise Service Center (ESC) was contracted by the OCFO to prepare the C&A package for CBIS. OPM's Senior Agency Information Security Officer reviewed the CBIS C&A package and signed the system's certification package on September 17, 2009. The system's Designated Accrediting Authority (OPM's Chief Information Officer) signed the accreditation statement and authorized the operation of the system on September 17, 2009.

II. FIPS 199 Analysis

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume I, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The CBIS security categorization analysis categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. CBIS is categorized with a moderate impact level for confidentiality, integrity, and availability, resulting in an overall categorization of moderate.

The security categorization of CBIS appears to be consistent with the guidance of FIPS 199 and NIST SP 800-60, and the OIG agrees with the categorization of moderate.

III. Information System Security Plan

The completion of an information system security plan (ISSP) is a requirement of OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources. In order to assist agencies in establishing a standardized approach to developing an ISSP, NIST developed SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems.

The ISSP for CBIS was created using the template outlined in NIST SP 800-18. The template requires that the following elements be documented within the ISSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Minimum Security Controls;
- Plan Completion Date; and
- Plan Approval Date.

The ISSP for CBIS was prepared in September 2009 and revised in August of 2010 in accordance with the format and methodology outlined in NIST SP 800-18. The CBIS ISSP contains the majority of the elements outlined by NIST SP 800-53 Revision 3 and NIST SP 800-18 Revision 1.

IV. <u>Risk Assessment</u>

A risk management methodology focused on protecting core business operations and processes is a key component of an efficient IT security program. A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

As part of the C&A process, ESC conducted a risk assessment of CBIS in September 2009 and evaluated the risk of each vulnerability in accordance with NIST SP 800-30 standards. NIST SP 800-30 offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) result documentation. Fifty-three vulnerabilities were identified during this assessment, and the following was documented for each one:

a. vulnerability description;
b. threat source;
c. existing controls;
d. likelihood, impact, and risk rating; and
e. control recommendations.

Each of these vulnerabilities was appropriately added to the CBIS Plan of Action and Milestones (POA&M) for tracking purposes (see section IX below).

V. Independent Security Control Testing

A security test and evaluation (ST&E) was completed for CBIS as a part of the system's C&A process in September 2009. The ST&E was conducted by ESC, an OPM contractor that was operating independently from the OCFO.

The OIG reviewed the controls tested by ESC to ensure that they included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

The ST&E labeled each security control as common (inherited from OPM's IT infrastructure), system-specific, or hybrid. The system specific and hybrid controls were tested as part of this ST&E, whereas the testing of common controls is the responsibility of OPM's Office of the Chief Information Officer (OCIO).

ESC tested 171 controls and determined that 19 controls were not adequately implemented. ESC presented a copy of the evaluation results to the OCFO, and each of the identified weaknesses was appropriately incorporated into the CBIS POA&M for tracking purposes.

VI. Security Control Self-Assessment

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent ST&E is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

The designated security officer for CBIS conducted a self-assessment of the system in September 2010. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Although the OCFO did not identify any weaknesses in the 150 security controls that were tested, an OIG test of security controls indicated that system weaknesses do exist (see section X, below).

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The OPM IT Security and Privacy Policy Volume 2 requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The CBIS Disaster Recovery (DR) plan documents the functions, operations, and resources necessary to restore and resume computer operations when unexpected events or disasters occur. The CBIS DR plan is reviewed and updated annually and contains the majority of elements recommended by NIST SP 800-34 guidelines, including:

- System background information;
- Concept of operations;
- Notification/activation phase;
- Recovery operations; and
- Procedures to return to normal operations.

Contingency Plan Test

NIST SP 800-34, Contingency Planning Guide for Information Technology, provides guidance for conducting and documenting contingency plan testing. Genuine Contingency plan testing is a critical element of a viable disaster response capability.

In March of 2010, the OCFO conducted its annual disaster recovery table top test. The test involved discussing the steps of restoring all mission critical functions after a temporary electrical outage. The documentation resulting from the CBIS DR test contains the majority of the items mentioned in the NIST guide including the scope, objectives, participants, and logistics.

The disaster recovery test summary documented potential problems that were discovered during or at the conclusion of the test. However, one recommendation identified during the 2010 DR test has not been added to the CBIS POA&M for tracking purposes (see section IX below).

VIII. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a screening or Privacy Threshold Analysis (PTA) of federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system.

OMB Memorandum M-03-22 outlines the necessary components of a PIA. A PIA is used to ensure that no collection, storage, access, use, or dissemination of personally identifiable information occurs that is not needed or authorized. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

The OCFO completed the PTA of CBIS and determined that a PIA was required for this system. A PIA was conducted for CBIS in May 2009. Although the CBIS PIA contained the majority of the elements of M-03-22, it did not address several requirements applicable to major information systems, including:

- The consequences of collection and flow of information;
- The alternatives to collection and handling as designed;
- The appropriate measures to mitigate risks identified for each alternative; and
- The rationale for the final design choice or business process.

This issue was originally identified during the OIG's 2009 audit of CBIS.

Recommendation 1 ***(Roll-forward from OIG Report 4A-CI-00-09-066 Recommendation 4)***

We continue to recommend that all OMB Memorandum 03-22 requirements are incorporated into the CBIS PIA.

OCFO- FSM Response:

"We concur with the OIG recommendation. We have addressed the citations that were noted in our recent CBIS PIA. Currently the PIA is under review by the CIO IT Security Office and based upon their approval or proposed actions, we will forward the revised version of [the] CBIS PIA to your office for review no later than April 30, 2011."

OIG Reply:

We acknowledge the steps that OCFO has taken to update the CBIS PIA; no further action is required.

IX. Plan of Action and Milestones Process

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The OIG evaluated the CBIS POA&M and verified that it follows the format of OPM's template, and has been routinely submitted to the OCIO for evaluation. However, we found that security weaknesses identified during CBIS DR testing and reviews conducted by the OIG and KPMG have not been added to the CBIS POA&M.

Recommendation 2

We recommend that the OCFO promptly update the CBIS POA&M to include all known security weaknesses.

OCFO- FSM Response:

***"We concur with the OIG recommendation and our objective is to develop a centralized toolset and/or utilize CIO's [redacted] to monitor and track all POA&M's/CAP regardless of the origin of the finding or recommendation. ….
We also concur that … four (4) POA&M's from the CBIS Disaster Recovery (DR) testing were omitted from the POA&M's listing but it is being tracked and monitored under the A-***

123 review process. After this review is completed (currently by the Policy and Internal Controls group), we will submit to your attention no later than April 30, 2011."

OIG Reply:

Although the OCFO uses a variety of tools to track CBIS security weakness, FISMA requires Federal agencies track all weaknesses using the standard POA&M template developed by the Office of Management and Budget. Use of the standardized POA&M template allows the OCIO to track security weaknesses for all of the agency's information systems.

In order to adequately address this recommendation the OCFO must add all known security weaknesses to the CBIS POA&M in addition to any other tracking tools used by the program office.

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, the OIG determined whether a subset of these controls had been adequately implemented for CBIS, including:

- AC-2 Account Management
- AC-4 Information Flow Enforcement
- AC-7 Unsuccessful Login Attempts
- AC-8 System Use Notification
- AC-11 Session Lock
- AC-13 Supervision and Review – Access Control
- AT-3 Security Training
- AU-2 Auditable Events
- AU-3 Content of Audit Records
- AU-6 Audit Review, Analysis, Reporting
- CA-3 Information System Connections
- CM-2 Baseline Configuration
- CM-6 Configuration Settings
- CP-6 Alternate Storage Site
- IA-2 Identification and Authentication
- IA-5 Authenticator Management
- IR-6 Incident Reporting
- MP-6 Media Sanitization and Disposal
- CP-9 Information System Backup
- PE-2 Physical Access Authorization
- PL-4 Rules of Behavior
- PS-4 Personnel Termination
- PS-7 Third-Party Personnel Security
- RA-5 Vulnerability Scanning
- SA-4 Acquisitions
- SC-10 Network Disconnect
- SI-10 Information Accuracy, Completeness, Validity, and Authenticity
- SI-11 Error Handling

These controls were evaluated by interviewing individuals with CBIS security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 security controls have been successfully implemented for CBIS, several tested controls were not fully satisfied.

a) (AC-2) Account Management

[redacted]

NIST SP 800-53 Control AC-2 requires an organization to review, disable, and remove user accounts when necessary.

[redacted]

Recommendation 3

We recommend that the OCFO [redacted]

OCFO -FSM Response:

"We concur with the [OIG] recommendation and are currently conducting our [redacted] ***We also acknowledge*** [redacted] ***A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011."***

"Even though we communicate the risk of [redacted]***. We recommend that for that situation we will identify a policy and procedures to establish a waiver that [transfers] the risk to the program offices."***

OIG Reply:

We acknowledge the steps taken by the OCFO to address this issue. In order to fully close this audit recommendation, we recommend that the OCFO provide IOC with evidence that [redacted] or that the risk was formally accepted by senior management from that user's program office.

Recommendation 4

We recommend that the OCFO [redacted]

OCFO-FSM Response:

"We concur with the [OIG] recommendation and are currently conducting our [redacted]

[redacted] A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011."

<u>OIG Reply:</u>

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence [redacted].

<u>Recommendation 5</u>

We recommend that the OCFO develop and implement a process to routinely audit [redacted]

<u>OCFO-FSM Response:</u>

"We concur with the [OIG] recommendation and we will continue to revise our CBIS account management guide to include the OIG audit recommendations, system enhancements and policies and procedures to improve the security management processes. More specifically, we will routinely review [redacted] We acknowledge that the security oversight for CBIS is [redacted] and we have made a recommendation to OCFO management to invest into a product similar to [redacted] that provides capabilities to assess and alert in cases where security violations have occurred. In the interim, we have developed reports that allow OPM Program Office [RMOs] and the CBIS security team a means to effectively monitor [redacted].

We recommend CBIS users and supervisors submit [redacted] directly to their Program Office RMO to obtain their approval and assist them in monitoring and tracking [redacted] A revised account management guide, [including] these refined policies, will be forwarded to OIG no later than April 30, 2011."

<u>OIG Reply:</u>

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence that it has implemented a process to routinely audit [redacted] s.

b) (AC-5) Segregation of Duties Issue

The OCFO developed a policy that describes specific user roles that cannot be assigned to a single individual in conjunction with other roles due to segregation of duty conflicts (e.g., one user having both payables manager and receivables manager roles). We reviewed the active roles of all current CBIS users and determined that 191 users had roles that violated the segregation of duties policy.

NIST SP 800-53 Control AC-5 states that system owners must separate duties of individuals as necessary to prevent malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

The OCFO informed the OIG that several of the users that have segregation of duties issues have a business need to have conflicting roles. If this is the case, then the CBIS segregation of duties policy is not accurate, further indicating that the OCFO does not have adequate controls regarding segregation of duties. We consider this weakness to be a significant deficiency in CBIS's IT security controls.

Recommendation 6

We recommend that the OCFO review (and update if necessary) the CBIS segregation of duties policy to ensure it accurately reflects business requirements.

OCFO-FSM Response:

"We concur with the [OIG] recommendation and we have refined the CBIS Segregation of Duties metric table (SoD Metric Table) to be reviewed by OIG. We are seeking OIG concurrence and approval to use this refined SoD as a basis for the internal control of user security of reducing the likelihood of fraud by discouraging collusion. If we receive concurrence, we will advise OPM Program Office [RMOs] and our security team of the newly refined SoD that will assist them in validating and executing user access requests accurately.

A revised account management guide, [including] these refined policies, will be forwarded to OIG no later than April 30, 2011."

OIG Reply:

We acknowledge the steps the OCFO has taken to refine the CBIS SoD metric table. However, the OIG is not in a position to approve the implementation of this new table, as the development of a SoD policy requires a detailed understanding of the business requirements specific to the application. Furthermore, the OIG is an independent oversight entity and cannot participate in the development of policies and procedures of the program offices we audit.

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence that it has updated the CBIS segregation of duties policy.

Recommendation 7

We recommend that the OCFO adjust the user roles for the accounts identified as having segregation of duties violations.

OCFO-FSM Response:

"We concur with the [OIG] recommendation and are currently conducting our semi-annual user account assessment [for] each OPM program office [of] their CBIS users. Utilizing the SoD Metric Table, we are advising OPM Program Office [RMOs] where role requests violate security standards and will recommend they re-assess requested roles based on the SoD.

We are aware that this refined policy will cause some concern within OPM organizations, so FSM is developing an annual CBIS Security Training Awareness to reinforce this and all other policy changes on a routine and continual basis. Any support from OIG that endorses these newly refined policies is appreciated. A revised account management guide, [including] these refined policies, will be forwarded to OIG no later than April 30, 2011."

"FSM assumes the responsibility for administration and execution of user account management. As such, we will establish a policy allowing a waiver (in extreme circumstances) to bypass the SoD conflicts. However, this waiver also transfers the risk to the OPM Program Office to ensure that actions performed within the system as a result of [the] waiver does not introduce or permit fraudulent transactions and use."

OIG Reply:

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence that it has adjusted the user roles for the accounts with segregation of duties violations.

Recommendation 8

We recommend that the OCFO modify the CBIS system so that technical controls are in place to prevent user accounts from being created with segregation of duties violations.

OCFO-FSM Response:

"We partially-concur with the [OIG] recommendation. To retrofit this recommendation would require the purchase of [redacted] ***has the functionality to determine and alert when security violations occur and to monitor system configurations and security set-ups. FSM is recommending the purchase of*** [redacted] ***to CFO leadership for consideration. Upon approval, it will be forwarded to the CBIS Change Control Board and the Executive Steering Committee for review and analysis. In the interim FSM's Financial Application Management (FAM) Group will continue to use SoD and other reports defined in our account management guidelines to monitor and track SoD violations. We will introduce a change request to both the CCB and then ESC for concurrence no later than April 30, 2011."***

<u>OIG Reply:</u>

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence that it has implemented technical controls to prevent user accounts from being created with segregation of duties violations.

<u>Recommendation 9</u>

We recommend that the OCFO implement a process to routinely audit all active user accounts to identify accounts that have roles that violate the segregation of duties policy.

<u>OCFO-FSM Response:</u>

"We concur with the [OIG] recommendation and we are developing security incident reports to assist the security team and OPM Program Office [RMOs] in conducting more frequent reviews of CBIS user accounts (within their organization) and to also alert when those accounts may violate the approved SOD Metrics. More specifically, we (the CBIS security team) will routinely review user accounts on a quarterly basis and when needed.

We recommend CBIS users and supervisors submit security access forms directly to their Program Office RMO to obtain their approval and assist them in monitoring and tracking modifications to user accounts. A revised account management guide, [including] these refined policies, will be forwarded to OIG no later than April 30, 2011."

<u>OIG Reply:</u>

As part of the audit resolution process we recommend that the OCFO provide IOC with evidence that it is routinely auditing CBIS user accounts to identify segregation of duties violations.

c) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Recommendation 10

[redacted]

OCFO-FSM Response:

"We concur with the [OIG] recommendation. [redacted]

[redacted]

OIG Reply:

[redacted]

Recommendation 11

We recommend that the appropriate technical modifications be made to CBIS to [redacted]

OCFO-FSM Response:

"We partially-concur with the [OIG] recommendation and [redacted]

[redacted]

[redacted] ***FSM is recommending the purchase of*** [redacted] ***to CFO leadership for consideration.***

[redacted]

OIG Reply:

We acknowledge the fact that [redacted] nce the [redacted] is complete, we recommend that the OCFO provide IOC with evidence that the [redacted]

Recommendation 12

We recommend that the OCFO [redacted]

OCFO-FSM Response:

"We partially-concur with the [OIG] recommendation [redacted]

1. Current Active users and assigned responsibilities

[redacted]

[redacted] ***FSM is recommending the purchase of*** [redacted] ***to CFO leadership for consideration.***

[redacted]

<u>OIG Reply:</u>

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence indicating that the program office [redacted] discussed in Recommendation 10, above.

d) (CM-6) Configuration Settings

The OIG conducted vulnerability scans of the [redacted] databases supporting CBIS using [redacted] scanning tool. The vulnerability scans revealed that the databases contained settings configured in a manner not fully compliant with best practices as defined by [redacted] Although the technical details of these settings will not be included in this report, the OCFO has been provided with this information.

NIST SP 800-53 Control CM-6 states that information systems should be configured in a manner that reflect the most restrictive mode consistent with operational requirements.

<u>Recommendation 13</u>

We recommend that the OCFO evaluate the potential configuration weaknesses identified by the OIG and, if necessary, make the appropriate technical modifications.

OCFO-FSM Response:

"We do not concur with the [OIG] recommendation. The results of the scan conducted by the OIG were anticipated and expectedly applicable to the CBIS database configuration. The scan conducted by OIG identified [items] … required for (and support) the CBIS [application's] day-to-day operations. … As such, we believe we are in compliance with NIST SP 800-53 Control CM-6 as the system is configured in a manner that restricts access based on the operational requirement … to support CBIS operations."

OIG Reply:

We acknowledge the fact that the configuration settings questioned are required to support CBIS day-to-day operations. No further action is required.

e) [redacted]

[redacted]

[redacted]

[redacted]

Recommendation 14

We recommend that the OCFO [redacted]

OCFO-FSM Response:

"We concur with the [OIG] recommendation and are currently conducting our [redacted]

FAM will ensure that the processes [redacted] ***A revised account management guide, [including] these refined policies, will be forwarded to OIG no later than April 30, 2011."***

OIG Reply:

As part of the audit resolution process, we recommend that the OCFO provide IOC with evidence indicating [redacted]

Recommendation 15

We recommend that the OCFO implement a process [redacted]

Recommendation 16

We recommend that the OCFO implement a procedure to [redacted].

OCFO-FSM Response:

"We concur with the [OIG] recommendation. FAM will request that CIO provides the CBIS security team [redacted] ***Upon implementation of this process, we will notify the OPM Program Office [RMOs] that they*** [redacted]

We will forward a revised account management guide that includes these refined policies for review no later than April 30, 2011."

OIG Reply:

We agree that the OCFO's plan to use the [redacted] owever, the intent of Recommendations 15 and 16 is to implement both [redacted]

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted], Auditor In Charge

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Financial
Officer

February 8, 2011

MEMORANDUM FOR [redacted]
Chief, Information Systems Audit Group

FROM: ROCHELLE S. BAYARD Rochelle Bayard
Associate Chief Financial Officer
Financial Systems Management (FSM)

SUBJECT: Management Response to Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Consolidated Business Information System – Report Number 4A-CF-00-11-015

We have reviewed your draft audit report on OPM's Consolidate Business Information System (CBIS) program and are in concurrence with majority of the findings and recommendations identified in the report. We recognize that even the most well run programs can benefit from an external evaluation and the input of the Office of the Inspector General indicates that after the first year, CBIS has delivered the business goal of safeguarding information against unauthorized use, disclosure or damage/loss of financial and procurement management data. CBIS security administration procedures are defined and fit into OPMs' structure for security policies and procedures, responsibilities for IT security are assigned, but we recognize that they are not consistently enforced. We will continue to work to enhance the CBIS procedures and practices to ensure the application's security processes are coordinated with the overall OPM security functions and with specific security baselines and measures. Our official management responses to your recommendations are provided below in **blue**.

<u>OIG Response to Recommendations 1- Privacy Impact Assessment</u>

OCFO completed the PTA of CBIS and determined that a PIA was required for this system. A privacy impact assessment (PIA) was conducted for CBIS in May 2009. Although the CBIS PIA contained the majority of the elements of M-03-22, it did not address several requirements applicable to major information systems, including:

- The consequences of collection and flow of information;
- The alternatives to collection and handling as designed;
- The appropriate measures to mitigate risks identified for each alternative; and
- The rationale for the final design choice or business process.

This issue was originally identified during the OIG's 2009 audit of CBIS.

Appendix

<u>OIG Recommendation 1</u> - (Roll-forward from OIG Report 4A-CI-00-09-066 Recommendation 4)

We continue to recommend that all OMB Memorandum 03-22 requirements be incorporated into the CBIS PIA.

FSM Management Response to Recommendation 1:

We concur with the OIG recommendation. We have addressed the citations that were noted in our recent CBIS PIA. Currently the PIA is under review by the CIO IT Security Office and based upon their approval or proposed actions, we will forward the revised version of CBIS PIA to your office for review no later than April 30, 2011.

<u>OIG Response to Recommendation 2- Plan of Action and Milestones Process</u>

The OIG evaluated the CBIS POA&M and verified that it follows the format of OPM's template, and has been routinely submitted to OCIO for evaluation. However, we found that security weaknesses identified during CBIS DR testing and reviews conducted by OIG and KPMG have not been added to the CBIS POA&M.

<u>OIG Recommendation 2</u>

We recommend that OCFO promptly update the CBIS POA&M to include all known security weaknesses.

FSM Management Response to Recommendation 2:

We concur with the OIG recommendation and our objective is to develop a centralized toolset and/or utilize CIO's [redacted] *to monitor and track all POA&M's/CAP regardless of the origin of the finding or recommendation. More importantly, we will receive recipient signature acknowledging the acceptance and submission of POA&Ms under review.*

We also concur that the following four (4) POA&M's from the CBIS Disaster Recovery (DR) testing were omitted from the POA&M's listing but it is being tracked and monitored under the A-123 review process. After this review is completed (currently by the Policy and Internal Controls Group), we will submit to your attention no later than April 30, 2011.

1. *CP-6.1: Alternate storage site agreement are not is place*
2. *CP-6.2: Primary storage site hazards are not defined within the CDRP*
3. *CP-3: Contingency training material has not been defined or documented*
4. *CP-9: System backup testing is not conducted*

<u>OIG Response to Recommendation 3 - (AC-2) Account Management</u>

[redacted].

NIST SP 800-53 Control AC-2 requires an organization to review, disable, and remove user accounts when necessary.

Appendix

[redacted].

OIG Recommendation 3

We recommend that OCFO [redacted].

FSM Management Response to Recommendation 3:

We concur with the IG recommendation and are currently conducting our [redacted] We also acknowledge that [redacted]. A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

OIG Response to Recommendation 4 -(AC-2) Account Management

[redacted].

NIST SP 800-53 Control AC-2 requires an organization to review, disable, and remove user accounts when necessary.

[redacted]

OIG Recommendation 4

[redacted].

FSM Management Response to Recommendation 4:

We concur with the IG recommendation and are currently conducting our [redacted]. Specifically, informing program office that [redacted]. Even though we communicate the risk of [redacted]. We recommend that for that situation we will identify a [redacted]. A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

OIG Response to Recommendation 5 -(AC-2) Account Management

[redacted].

NIST SP 800-53 Control AC-2 requires an organization to review, disable, and remove user accounts when necessary.

[redacted]

OIG Recommendation 5

We recommend that OCFO develop and implement a process to [redacted].

FSM Management Response to Recommendation 5:

We concur with the IG recommendation and we will continue to revise our CBIS account management guide to include the OIG audit recommendations, system enhancements and policies and procedures to improve the security management processes. More specifically, we will [redacted] *We acknowledge that the security oversight for CBIS is* [redacted] *and we have made a recommendation to OCFO management to invest into a product similar to* [redacted] *that provides capabilities to assess and alert in cases where security violations have occurred. In the interim, we have developed reports that allow OPM Program Office RMO's and the CBIS security team a means to effectively monitor* [redacted].

We recommend CBIS users and supervisors submit [redacted] *directly to their Program Office RMO to obtain their approval and assist them in monitoring and tracking* [redacted]. *A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.*

OIG Response to Recommendation 6 - (AC-5) Segregation of Duties Issue Management

OCFO developed a policy that describes specific user roles that cannot be assigned to a single individual in conjunction with other roles due to segregation of duty conflicts (e.g., one user having both payables manager and receivables manager roles). We reviewed the active roles of all current CBIS users and determined that 191 users had roles that violated the segregation of duties policy.

NIST SP 800-53 control AC-5 states that system owners must separate duties of individuals as necessary to prevent malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

OCFO informed OIG that several of the users that have segregation of duties issues have a business need to have conflicting roles. If this is the case, then the CBIS segregation of duties policy is not accurate, further indicating that OCFO does not have adequate controls regarding segregation of duties. We consider this weakness to be a significant deficiency in CBIS' IT security controls.

Appendix

OIG Recommendation 6

We recommend that the OCFO review (and update if necessary) the CBIS segregation of duties policy to ensure it accurately reflects business requirements.

FSM Management Response to Recommendation 6:

We concur with the IG recommendation and we have refined the CBIS Segregation of Duties metric table (SoD Metrics Table) to be reviewed by OIG. We are seeking OIG concurrence and approval to use this refined SoD as a basis for the internal control of user security of reducing the likelihood of fraud by discouraging collusion. If we receive concurrence, we will advise OPM Program Office RMO's and our security team of the newly refined SoD that will assist them in validating and executing user access requests accurately.

FSM assumes the responsibility for administration and execution of user account management. As such, we will establish a policy allowing a waiver (in extreme circumstances) to bypass the SoD conflicts. However, this waiver also transfers the risk to the OPM Program Office to ensure that actions performed within the system as o result of waiver does not introduce or permit fraudulent transactions and use. A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

Response to Recommendation 7 - (AC-5) Segregation of Duties Issue Management

OCFO developed a policy that describes specific user roles that cannot be assigned to a single individual in conjunction with other roles due to segregation of duty conflicts (e.g., one user having both payables manager and receivables manager roles). We reviewed the active roles of all current CBIS users and determined that 191 users had roles that violated the segregation of duties policy.

NIST SP 800-53 control AC-5 states that system owners must separate duties of individuals as necessary to prevent malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

OCFO informed OIG that several of the users that have segregation of duties issues have a business need to have conflicting roles. If this is the case, then the CBIS segregation of duties policy is not accurate, further indicating that OCFO does not have adequate controls regarding segregation of duties. We consider this weakness to be a significant deficiency in CBIS' IT security controls

OIG Recommendation 7

We recommend that OCFO adjust the user roles for the accounts identified as having segregation of duties violations.

FSM Management Response to Recommendation 7:

We concur with the IG recommendation and are currently conducting our semi-annual user account assessment of each OPM program office for their CBIS users. Utilizing the SoD Metric Table, we are advising OPM Program Office RMO's where role requests violate security standards and will recommend they re-assess requested roles based on the SoD.

We are aware that this refined policy will cause some concern within OPM organizations, so FSM is developing an annual CBIS Security Training Awareness to reinforce this and all other policy changes on a routine and continual basis. Any support from OIG that endorses these newly refined policies is appreciated. A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

Response to Recommendation 8 - (AC-5) Segregation of Duties Issue Management

OCFO developed a policy that describes specific user roles that cannot be assigned to a single individual in conjunction with other roles due to segregation of duty conflicts (e.g., one user having both payables manager and receivables manager roles). We reviewed the active roles of all current CBIS users and determined that 191 users had roles that violated the segregation of duties policy.

NIST SP 800-53 control AC-5 states that system owners must separate duties of individuals as necessary to prevent malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

OCFO informed OIG that several of the users that have segregation of duties issues have a business need to have conflicting roles. If this is the case, then the CBIS segregation of duties policy is not accurate, further indicating that OCFO does not have adequate controls regarding segregation of duties. We consider this weakness to be a significant deficiency in CBIS' IT security controls

OIG Recommendation 8

We recommend that OCFO modify the CBIS system so that technical controls are in place to prevent user accounts from being created with segregation of duties violations.

FSM Management Response to Recommendation 8:

We partially-concur with the IG recommendation. To retrofit this recommendation would require the purchase of [redacted] that has the functionality to determine and alert when security violations occur and to monitor system configurations and security set-ups. FSM is recommending the purchase of this [redacted] to CFO leadership for consideration. Upon approval, it will be forwarded to the CBIS Change Control Board and the Executive Steering Committee for review and analysis. In the interim FSM's Financial Application Management (FAM) Group will continue to use SoD and other reports defined in our account management guidelines to monitor and track SoD violations. We will introduce a change request to both the CCB and then ESC for concurrence no later than April 30, 2011.

Response to Recommendation 9 - (AC-5) Segregation of Duties Issue Management

OCFO developed a policy that describes specific user roles that cannot be assigned to a single individual in conjunction with other roles due to segregation of duty conflicts (e.g., one user having both payables manager and receivables manager roles). We reviewed the active roles of all current CBIS users and determined that 191 users had roles that violated the segregation of duties policy.

NIST SP 800-53 control AC-5 states that system owners must separate duties of individuals as necessary to prevent malevolent activity without collusion. Failure to implement adequate separation of duties increases the risk that malicious activity by system users remains undetected.

OCFO informed OIG that several of the users that have segregation of duties issues have a business need to have conflicting roles. If this is the case, then the CBIS segregation of duties policy is not accurate, further indicating that OCFO does not have adequate controls regarding segregation of duties. We consider this weakness to be a significant deficiency in CBIS' IT security controls

OIG Recommendation 9

We recommend that OCFO implement a process to routinely audit all active user accounts to identify accounts that have roles that violate the segregation of duties policy.

FSM Management Response to Recommendation 9:

We concur with the IG recommendation and we are developing security incident reports to assist the security team and OPM Program Office RMO's in conducting more frequent reviews of CBIS user accounts (within their organization) and to also alert when those accounts may violate the approved SoD Metrics. More specifically, we (the CBIS security team) will routinely review user accounts on a quarterly basis and when needed.

We recommend CBIS users and supervisors submit security access forms directly to their Program Office RMO to obtain their approval and assist them in monitoring and tracking modifications to user accounts. A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

Response to Recommendation 10[redacted]

[redacted]

[redacted]

[redacted]

Appendix

[redacted]

[redacted].

<u>OIG Recommendation 10</u>

[redacted]

FSM Management Response to Recommendation 10:

We concur with the IG recommendation. [redacted]. *A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.*

[redacted]

<u>Response to Recommendation 11</u> [redacted]

OCFO does not have any policies or procedures related to [redacted].

We requested from OCFO a list [redacted]

[redacted]

[redacted].

<u>OIG Recommendation 11</u>

We recommend that the appropriate technical modifications be made to CBIS to [redacted]

Appendix

FSM Management Response to Recommendation 11:

We partially-concur with the IG recommendation and [redacted]

[redacted]

[redacted]

[redacted]

[redacted]*n the meantime, we will continue to make use of* [redacted] *procedure in our revised account management guide for your review no later than April 30, 2011.*

Response to Recommendation 12 [redacted]

[redacted]

[redacted]

[redacted]

[redacted].

OIG Recommendation 12

We recommend that OCFO [redacted].

Appendix

FSM Management Response to Recommendation 12:

We partially-concur with the IG recommendation [redacted]

[redacted]

[redacted].

FSM is recommending the purchase of this [redacted] *to CFO leadership for consideration.*

In the meantime, we will continue to make use of [redacted] *procedure in our revised account management guide for your review no later than April 30, 2011.*

Response to Recommendation 13 (CM-6) Configuration Settings

The OIG conducted vulnerability scans of the [redacted] databases supporting CBIS using the [redacted]. The vulnerability scans revealed that the databases contained settings configured in a manner not fully compliant with best practices as defined by [redacted] Although the technical details of these settings will not be included in this report, OCFO has been provided with this information.

NIST SP 800-53 control CM-6 states that information systems should be configured in a manner that reflect the most restrictive mode consistent with operational requirements.

OIG Recommendation 13

We recommend that OCFO evaluate the potential configuration weaknesses identified by the OIG and, if necessary, make the appropriate technical modifications.

FSM Management Response to Recommendation 13:

We do not concur with the IG recommendation. The results of the scans conducted by the OIG were anticipated and expectedly applicable to the CBIS database configuration. The scan conducted by OIG identified [redacted] *that upon review are required for (and support) the CBIS applications day-to-day operations. Part of the base* [redacted] *install requires a direct database login and this access is granted only to the CBIS Database Administrators (DBAs). As such, we believe we are in compliance with NIST SP 800-53* *control CM-6 as the system is configured in a manner that restricts access based on the operational requirement which provides DBA's only this type of access to support CBIS operations.*

Response to Recommendation 14 [redacted]

[redacted].

[redacted]

[redacted].

OIG Recommendation 14

We recommend that OCFO [redacted]

FSM Management Response to Recommendation 14:

We concur with the IG recommendation and are currently conducting our [redacted].

FAM will ensure that the processes used to [redacted]. *A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.*

Response to Recommendation 15 [redacted]

[redacted]

[redacted]

[redacted].

Appendix

OIG Recommendation 15

We recommend that the OCFO [redacted].

FSM Management Response to Recommendation 15:

We concur with the IG recommendation. FAM will request that CIO provides the CBIS security team [redacted]. Upon implementation of this process, we will notify the OPM Program Office RMO's that they [redacted].

As a part of an security overview notification to OPM Program Office RMO's, the CBSI security team will require RMO's to ensure that [redacted] We will forward a revised account management guide that includes these refined policies for review no later than April 30, 2011.

Response to Recommendation 16 [redacted]

[redacted]

[redacted]

[redacted].

OIG Recommendation 16

We recommend that the OCFO implement a procedure to [redacted]

FSM Management Response to Recommendation 16:

We concur with the IG recommendation. FAM will request that CIO provides the CBIS security team [redacted]. Upon implementation of this process, we will notify the OPM Program Office RMO's that they [redacted]

A revised account management guide, to include these refined policies, will be forwarded to OIG no later than April 30, 2011.

Appendix

cc:

Daniel Marella *(Deputy Chief Financial Officer)*
Mark Lambert (*Director Internal Oversight and Compliance*)
Janet Barnes (*Deputy Director, Internal Oversight and Compliance)*
[redacted] (*Chief, CFO/FSM/ Financial Application Management*)
[redacted] (*Acting Chief, CFO/Policy and Internal Controls)*