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

Final Audit Report

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

Report Number 4A-CF-00-19-026
October 3, 2019

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Consolidated Business Information System

Report No. 4A-CF-00-19-026 **October 3, 2019**

Why Did We Conduct The Audit?

The Consolidated Business Information System (CBIS) is one of the U.S. Office of Personnel Management's (OPM) major information technology (IT) systems. The Digital Accountability and Transparency Act of 2014 and the Federal Information Security Modernization Act (FISMA) require that the Office of the Inspector General (OIG) perform audits of IT security controls of agency systems.

What Did We Audit?

The OIG completed a performance audit of CBIS to ensure that the system's security controls meet the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of CBIS determined that:

- A Security Assessment and Authorization (Authorization) was completed in May 2017. The Authorization was granted for up to three years.
- The CBIS security categorization is consistent with both the Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the "moderate" categorization.
- OPM has completed a Privacy Impact Assessment for CBIS.
- The CBIS System Security Plan was complete and follows the OCIO's template.
- An independent security assessment was performed prior to the Authorization being granted.
- Continuous Monitoring for CBIS was conducted in accordance with the agency's quarterly schedule for fiscal year 2018.
- The CBIS contingency plan and test are in compliance with NIST SP 800-34, Revision 1, and OCIO guidance.
- The CBIS Plan of Action and Milestones documentation is up to date and contains all identified weaknesses.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined most of the security controls tested appear to be in compliance; however, we did note several areas for improvement.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
CBIS	**Consolidated Business Information System**
CIS	**Center for Internet Security**
DATA Act	**Digital Accountability and Transparency Act of 2014**
DISA	**Defense Information Systems Agency**
ESC	**Enterprise Services Center**
FAA	**Federal Aviation Administration**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
HSPD-12	**Homeland Security Presidential Directive 12**
IR	**Incident Response**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCFO	**Office of the Chief Financial Officer**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIV	**Personal Identity Verification**
POA&M	**Plan of Action and Milestones**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

APPENDIX: OPM's August 28, 2019, response to the draft audit report, issued August 9, 2019.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

The 2002 Federal Information Security Management Act requires: (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. The 2014 Federal Information Security Modernization Act (FISMA) reaffirmed the objectives of the prior Act.

The 2014 Digital Accountability and Transparency Act of 2014 (DATA Act) requires the Office of the Inspector General (OIG) to: (1) review a statistically valid sampling of the spending data submitted under the DATA Act by the Federal agency; and (2) submit to Congress and make publically available a report assessing the completeness, timeliness, quality, and accuracy of the data sampled and the implementation and use of data standards by the Federal agency. In accordance with the DATA Act, we conducted an evaluation of the U.S. Office of Personnel Management (OPM)'s systems, processes, and internal controls in place over financial data management.

OPM's Consolidated Business Information System (CBIS) is used by the Office of the Chief Financial Officer (OCFO) to manage the financial resources and obligations of OPM. CBIS's functionality includes management of the agency's general ledger, accounts payable, accounts receivable, purchasing, procurement, and budgeting processes. CBIS is one of the agency's major information technology (IT) systems and a key system providing data for DATA Act reporting. As such, the DATA Act requires that the OIG perform an audit of the IT security controls of this system.

This was our third audit of the IT security controls for CBIS. The previous audits resulted in findings and recommendations documented in Report Numbers 4A-CI-00-11-015 and 4A-CF-00-17-043, dated June 1, 2011, and September 29, 2017, respectively. All of the recommendations from the previous audits have been closed.

OPM's Office of the Chief Information Officer (OCIO) and OCFO, in conjunction with the Federal Aviation Administration (FAA), share responsibility for implementing and managing the information technology (IT) security controls of CBIS. We discussed the results of our audit with the OCIO and OCFO representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an audit of the security controls for CBIS to ensure that the OCIO implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, and OPM's OCIO.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements were implemented for CBIS, including:

- Security Assessment and Authorization;
- Federal Information Processing Standards Publication 199 (FIPS 199) Analysis;
- Privacy Impact Assessment;
- System Security Plan (SSP);
- Security Assessment Plan and Report;
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Plan of Action and Milestones (POA&M) Process; and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the Generally Accepted 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 security controls and FISMA compliance efforts of OPM officials responsible for CBIS, including the evaluation of IT security controls in place as of July 2019.

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 objective.

To accomplish our objective, we interviewed representatives of OPM's OCIO and OCFO, as well as FAA representatives with security responsibilities for CBIS, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also 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 "Audit Findings and Recommendations" 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 the internal controls as a whole. The criteria used in conducting this audit includes:

- OPM Security Assessment and Authorization Guide;
- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;

- NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;

- Payment Card Industry Data Security Standard Requirement Version 3.2; 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, we conducted the audit in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended, performed the audit. We conducted the audit from April 2019 through July 2019 at OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's management of CBIS is consistent with applicable standards. While generally compliant, with respect to the items tested, OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY ASSESSMENT AND AUTHORIZATION

A Security Assessment and Authorization (Authorization) includes: 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I, mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. However, OPM does not yet have a mature program in place to continuously monitor system security controls, therefore an Authorization is required for all OPM systems at least once every three years as required by OPM policy.

CBIS was authorized to operate in May 2017. The Authorization is valid for up to three years and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

CBIS was authorized to operate in May 2017.

Nothing came to our attention to indicate that the CBIS Authorization was inadequate.

B. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. FIPS 199 provides guidance on how to assign appropriate categorization levels for information security according to a range of risk levels.

NIST SP 800-60, Revision 1, Volume II, 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 199.

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

The security categorization of CBIS appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and we agree with the categorization of "moderate."

Nothing came to our attention to indicate that the CBIS security categorization was inadequate.

C. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis of Federal information systems to determine if a Privacy Impact Assessment is required for that system. In accordance with OPM policies requiring annual review and approval, the CBIS Privacy Threshold Analysis was reviewed and approved by OPM's Office of Privacy and Information Management in February 2019. The analysis indicated a Privacy Impact Assessment is required due to the sensitivity of the data.

OMB Memorandum M-03-22 outlines the necessary components of a Privacy Impact Assessment. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system. In accordance with OMB and OPM requirements, the Privacy Impact Assessment was last updated and approved by the OPM Privacy Office in April 2017, at the time of the Authorization.

We did not detect any issues with the Privacy Impact Assessment performed on CBIS.

D. SYSTEM SECURITY PLAN

Federal agencies must implement, for each information system, the security controls outlined in NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a System Security Plan (SSP) for each system, and provides guidance for doing so.

The OCFO developed the CBIS SSP using the OCIO's SSP template which uses NIST SP 800-18, Revision 1, as guidance. The template requires the SSP to contain the following elements:

- System Name and Identifier;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- General Description/Purpose;
- Information System Type;

- System Environment;
- System Categorization;
- Security Control Selection;
- Completion and Approval Dates.
- System Interconnection/Information Sharing;
- Minimum Security Controls;
- Laws, Regulations, and Policies Affecting the System; and

We reviewed the current CBIS SSP, last updated in August 2018, and determined that it adequately reflects the system's current state. Nothing came to our attention to indicate that the CBIS SSP has not been properly documented and approved.

E. SECURITY ASSESSMENT PLAN AND REPORT

A Security Assessment Plan describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls.

The CBIS Security Assessment Plan and Security Assessment Report were created by the OCIO Information System Security Officer in March 2017 and April 2017, respectively. An independent assessment was conducted for the Authorization in May 2017.

During the prior audit, we found issues with the CBIS risk assessment missing controls that are required to be assessed for a moderate system. However, OPM has provided evidence the identified weaknesses were addressed; we support closure of the former recommendation.

OPM provided evidence to support closure of the 2017 recommendation.

Nothing came to our attention to indicate that the CBIS Security Assessment Plan and Report were inadequate.

F. CONTINUOUS MONITORING

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous Monitoring Plan template to each individual system's specific security control needs and then test the system's

security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

We received the fiscal year 2018 quarterly continuous monitoring submissions for CBIS. A review of the submissions revealed that over 160 distinct controls were tested.

Nothing came to our attention to indicate that the CBIS continuous monitoring process was inadequate.

G. CONTINGENCY PLANNING AND CONTINGENCY PLAN TESTING

NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

1. Contingency Plan

The CBIS contingency plan, signed in April 2018, documents the functions, operations, and resources necessary to restore and resume CBIS when unexpected events or disasters occur. The contingency plan follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans.

We did not detect any issues with the CBIS contingency plan.

2. Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans for all systems be tested annually to evaluate the plan's effectiveness and the organization's readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

The CBIS contingency plan test was conducted in December 2018. The test consisted of a failover to the disaster recovery environment for technical verification and to test server recovery capabilities.

Nothing came to our attention to indicate that the CBIS contingency plan testing process was inadequate.

H. PLAN OF ACTION AND MILESTONES PROCESS

A Plan of Action and Milestones (POA&M) is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for known 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.

During the previous audit of CBIS, we found that the system had incomplete POA&M documentation as well as overdue POA&Ms. However, the identified issues have since been remediated. The CBIS POA&M is properly formatted according to OPM policy and all weaknesses are properly documented, to include attainable closure dates.

We did not detect any issues with the CBIS POA&M.

I. NIST SP 800-53 EVALUATION

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the Federal government. As part of this audit, we evaluated whether OPM has implemented a subset of these controls for CBIS. We tested approximately 40 controls as outlined in NIST SP 800-53, Revision 4, including one or more controls from each of the following control families:

- Access Control;
- Audit and Accountability;
- Awareness and Training;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Incident Response;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Information Integrity; and
- System and Services Acquisition.

These controls were evaluated by interviewing individuals with system security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system. We determined that the majority of the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements, with the exceptions detailed below.

1. Control AT-3 – Role-Based Security Training

Currently, OPM does not provide or require role-based security training for CBIS personnel.

NIST SP 800-53, Revision 4, requires for moderate systems, that "The organization provides role-based security training to personnel with assigned security roles and responsibilities … ." NIST explains this can include, but is not limited to, "enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, [and] security control assessors." Additionally, NIST explains that training should include "adequate security-related technical training specifically tailored for their assigned duties … [and should occur] before authorizing access to the information system or performing assigned duties[,] … [w]hen required by information system changes[,] and … thereafter."

OPM requires all agency employees to complete annual security/privacy awareness training; however, this differs from role-based security training. Role-based security training should be tailored to the individual's assigned responsibilities and system access.

Furthermore, OPM's Security and Privacy Awareness and Training Policy requires system owners to "Provide role-based security and privacy training to OPM information system users responsible for the operation of security functions/mechanisms for systems under his or her portfolio."

Failure to provide role-based security training for the CBIS personnel with system level access, especially after significant changes to the system, increases the likelihood of user error, possibly exposing the system to additional risks.

Recommendation 1

We recommend that OPM provide and document role-based security training for CBIS personnel with system level access.

OPM Response:

"We partially concur with the recommendation that CBIS personnel did not provide adequate role-based security training as it relates to system level access. OPM currently tracks the specialized training requirements for users with privilege/system level roles and responsibilities. We acknowledge the need to provide additional guidance to CBIS security personnel and to effectively track system level specialized security training."

OIG Comment:

Role-based security training should be planned and tailored both to the CBIS system and the individual's role. This required level of job specific training would not be addressed by the agency's annual IT Security Awareness Training, nor fully addressed by the agency's specialized training hourly requirements for users with privileged system access, and should be tailored to the individuals' access to CBIS.

As part of the audit resolution process, we recommend that the agency provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement also applies to all subsequent recommendations in this audit report that OPM agrees to implement.

2. Control CM-6 – Configuration Settings

Documented baseline configuration settings are not defined for the CBIS operating systems. Baselines have not been defined by the agency. FAA previously scanned CBIS for Center for Internet Security standard compliance but switched to Defense Information Systems Agency standards without documenting approved settings nor allowed exceptions.

NIST SP 800-53, Revision 4, requires that the organization "Establishes and documents configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operation requirements … ."

Failure to document standard configuration settings for all information systems increases the risk of insecurely configured systems, which can lead to system exploitation.

Recommendation 2

We recommend that the OCFO work with FAA to implement standard security configuration settings for all operating platforms in use by CBIS.

OPM Response:

"[We] [d]o not concur. [The OCFO] disagrees with the recommendation that concludes documented baseline configuration settings are not defined for the CBIS operating systems.

In [FY 2017] (May 2017), OPM successfully completed the CBIS Lift and Shift project which migrated the CBIS environment to the FAA Enterprise Services Center (ESC). As a part of the 'lift and shift' effort, OPM inherited and agreed to [Center for Internet Security (CIS) benchmark] as the standard compliance to safeguard its financial management application against cyber threats. To ensure the integrity of hardware and software configurations, we required the establishment and maintenance of an accurate and complete configuration repository which is captured within [redacted]. The process includes collecting initial configuration information, establishing baselines to monitor and record all assets and changes to assets. There is a full integration of interrelated processes, and they are used to update configuration data in an automated fashion. Monthly vulnerability scans for application servers and semiannual scans for CBIS database servers are performed where physical verifications are applied and any deviations are corrected. Without this baseline configuration, the execution of vulnerability scans for anomalies would be unattainable for OPM's [Chief Information Officer] review of the integrity of configuration data.

The alternative analysis regarding the transition from CIS [benchmark] to [Defense Information Systems Agency (DISA) Security Technical Implementation Guide] as a standard configuration in the FAA ESC data center [has] been documented. The implementation schedule transitioning from CIS to DISA is expected to be completed in Q1 of FY 2020. CBIS continues to remain under the CIS configuration until production deployment of DISA."

OIG Comment:

Over the course of the audit, we did not receive any evidence that a documented configuration settings baseline is in place for CBIS. We were informed that CBIS was originally configured using CIS configuration standards. However, during fieldwork, FAA, the entity responsible for maintaining the configuration standard, stated that DISA is the current configuration standard for CBIS and formally responded to information requests indicating that there was no documented CBIS CIS baseline settings.

Additionally, OPM's management response addresses the standard for [redacted] servers, but fails to identify an intended configuration standard for the [redacted] servers or the [redacted] servers. All operating systems should have a defined configuration benchmark and scans should be tailored to audit against the configuration to ensure there are no unauthorized changes to system settings.

We continue to recommend that OPM work with FAA to establish and implement standard security configuration settings for all operating platforms in use by CBIS.

3. Control IA-2(12) – Acceptance of PIV Credentials

The CBIS Application does not enforce Personal Identity Verification (PIV) authentication. Users currently log in via username and password.

NIST SP 800-53, Revision 4, states that "In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also [must] employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security." OMB Memorandum M-11-11 also required all Federal information systems to uses Personal Identity Verification credentials for multi-factor authentication.

OPM has not allocated the necessary resources to address the OMB requirement for [redacted]. If the CBIS application was configured to only allow PIV authenticated users, an attacker would have an increased difficulty gaining access to sensitive data without possession of an authorized user's PIV credential.

Recommendation 3

We recommend that the CBIS application meet the requirements of OMB M-11-11 by requiring multi-factor authentication using PIV credentials.

OPM Response:

"We concur. We recognize that CBIS is unable to comply with Homeland Security Presidential Directive 12 (HSPD-12) that calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. In May 2019, [the] OCFO developed a feasibility study to examine the possibility of implementing this security requirement. CBIS is currently preparing to enter the migration implementation stage for transitioning to FAA's ESC's shared service financial management platform. CBIS sponsor and stakeholders approved the business functional and technical requirements, and feasibility study reports performed in accordance of [U.S. General Services Administration], Unified Shared Service Management's Modernization and Migration Management Playbook … Engagement/Discovery stages. As a part of the implementation stage in its migration to the FAA ESC's Delphi solution, OPM plans to incorporate the requirements of the HSPD-12 directive. This represents [the] OCFO's course of action to adhere to security standards under OMB 11-11 and HSPD-12."

4. Control IR-02 – Incident Response Training

OPM and FAA confirmed incident response training is not performed for CBIS despite the SSP stating that the control is inherited from FAA. FAA Information System Security Officers perform incident response training for other applications they support, but it is not performed for the CBIS application. Additionally, OPM system administrators do not perform incident response training specific to the CBIS application.

NIST SP 800-53, Revision 4, requires that the organization "provides incident response training to information system users consistent with assigned roles and responsibilities … ." Failure to perform incident response training can increase the remediation time for an incident which could render user data vulnerable.

Recommendation 4

We recommend that OPM ensure system administrators receive incident response training for CBIS.

OPM Response:

"We partially concur with the intent of the underlying finding, however we do not agree with the portion that pertains to IR-02 as it is an Agency Common Security Control which CBIS inherits from OPM. Incident Response (IR) training is covered in the annual Security Awareness Training which is completed by all CBIS personnel included system administrators. In addition, CBIS Financial Operations Management … conducts IR training as part of their annual Disaster Recovery Exercise in conjunction with ESC-[Enterprise Data Center] FAA personnel.

We are aware the IR training should be a part of all system admin specialized training and will work with [the] OCFO to ensure additional IR training is being performed outside of the Annual Security Awareness Training."

OIG Comment:

We do not agree that incident response training, required by NIST 800-53, Revision 4, control IR-02, is fully addressed by OPM's annual Security Awareness Training, as NIST requires training be "consistent with assigned roles and responsibilities …" for the system. Incident response training for CBIS should be tailored to the system and tracked by the System Owner.

Additionally, during fieldwork the OCFO stated that "FAA/ESC does not perform the [Information System Security Officer] work for the CBIS environment. [The Information System Security Officer's] hold [incident response training] for other applications they support, but not for the CBIS environment."

5. Control SA-22 – Unsupported Software Component

CBIS uses an unsupported software component, which is highly vulnerable. CBIS cannot operate without this software, which has been end of life for almost seven years. OPM has performed a risk analysis and plans to transition to a supported

Required software has been end of life and unsupported for almost seven years.

platform maintained by FAA. However, these efforts have been halted, awaiting approval from OMB and the Department of the Treasury. OPM has drafted a risk acceptance but it has not been approved. There is no timetable to upgrade the unsupported system component.

NIST SP 800-53, Revision 4, requires that an organization "Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer." NIST also requires that the organization, "Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs."

Failure to upgrade system software leaves information systems open to known vulnerabilities without any remediation available.

Recommendation 5

We recommend that OPM maintain an approved risk acceptance for the unsupported software until the system is transitioned to a supported platform.

OPM Response:

"We concur. Management accepts the risk of utilizing unsupported [redacted] software that supports OPM's procurement operations. [The] OCFO submitted to [the Chief Information Officer] a draft Risk Acceptance Waiver which is undergoing the final review and signature process. Upon completion, [the Chief Information Officer] will provide the completed documentation to [Internal Oversight and Compliance]."

Recommendation 6

We recommend that OPM remove or update the unsupported software from its environment.

OPM Response:

"We concur. We recognize that the procurement system utilizes an unsupported version [redacted] (version [redacted]). However, the [redacted] application configuration settings are only operable in the [redacted]. In May 2019, OCFO completed its Discovery stage in preparation for migrating its financial management processes to FAA's ESC Delphi solution. OPM plans to leverage the FAA ESC's upgraded technology strategy for its financial management and procurement business applications. This

represents [the] OCFO's course of action to ensure its systems (to include the procurement application) is in line with the required government defined IT architecture and technology standards."

6. Multi-factor Authentication to Datacenter

We performed a datacenter tour in June 2019 and found most physical and environmental controls mandated by NIST 800-53, Revision 4, to be in place. However, the FAA facility does not require multi-factor authentication to access the datacenter.

Multi-factor authentication is an industry-wide best practice for securing datacenter access. This is especially true in the financial field, as evident by the Payment Card Industry Data Security Standard Requirement, Version 3.2, requiring "multi-factor authentication for all non-console access into the card data environment for personnel with administrative access."

Failure to enforce multi-factor authentication increases the risk of unauthorized access to personally identifiable information and payment card information.

Recommendation 7

We recommend that the OCFO ensure enforcement of multi-factor authentication at the CBIS datacenter for non-console access.

OPM Response:

"We partially concur as acknowledged in recommendation #3 that the CBIS application does not enforce PIV authentication at the application level where credit card information would be stored. [The] OCFO's course of action to adhere to security standards under OMB 11-11 and HSPD-12, is by transitioning CBIS to the FAA ESC Delphi financial management solution.

However, OPM does not believe a weakness exists with the procedures to authenticate access to the ESC data center. FIPS 199 impact levels designates CBIS as a moderate system for confidentially, integrity and availability. Under the NIST SP 800-53 statute [PE-2 Physical Access Authorizations control], a moderate system is not required for multifactor authentication for physical access. In compliance with FISMA and [Department of Transportation]/FAA regulations, ESC-[Enterprise Data Center] deploys NIST SP 800-53 physical security controls.

The observation reference Payment Card Industry Data Security Standards …, which is an information security standard for organizations that handle branded credit cards from the major card schemes, does not relate to NIST regulations regarding to 'non-console access into the data environment'."

OIG Comment:

We acknowledge that the FIPS 199 impact level designates CBIS as a moderate system. We also acknowledge that NIST does not designate control PE-2(2) as a control that is required for a moderate system. However, our audit criteria is not restricted to NIST. Payment Card Industry Data Security Standard provides the industry best practice for handling of credit card information. CBIS maintains encrypted credit card information in it's data environment. Therefore, we identified a need for more safeguards in the form of multi-factor authentication into the datacenter space to protect user credit card information.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Financial
Officer

August 28, 2019

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audits Group

FROM: DENNIS S. COLEMAN
Chief Financial Officer

CLARE A. MARTORANA
Chief Information Officer

SUBJECT: Audit of the Information Technology Security Controls of the Office of personnel Management's Consolidated Business Information System Report Number - 4A-CF-00-19-026

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the Office of Personnel Management's Consolidated Business Information System, Report Number 4A-CF-00-19-026, dated August 9, 2019.

Responses to your recommendations including planned corrective actions, as appropriate, are provided below.

Recommendation 1: We recommend that OPM provide and document role-based security training for CBIS personnel with system level access.

Management Response: We partially concur with the recommendation that CBIS personnel did not provide adequate role-based security training as it relates to system level access. OPM currently tracks the specialized training requirements for users with privilege/system level roles and responsibilities. We acknowledge the need to provide additional guidance to CBIS security personnel and to effectively track system level specialized security training.

Recommendation 2: We recommend that OCFO work with FAA to implement standard security configuration settings for all operating platforms in use by CBIS.

Management Response: Do not concur. CFO disagrees with the recommendation that concludes documented baseline configuration settings are not defined for the CBIS operating systems.

In FY17 (May 2017), OPM successfully completed the CBIS Lift and Shift project which migrated the CBIS environment to the FAA Enterprise Services Center (ESC). As a part of the 'lift and shift' effort, OPM inherited and agreed to CIS as the standard compliance to safeguard its financial management application against cyber threats. To ensure the integrity of hardware and software configurations, we required the establishment and maintenance of an accurate and complete configuration repository which is captured within [redacted]. The process includes collecting initial configuration information, establishing baselines to monitor and record all assets and changes to assets. There is a full integration of interrelated processes, and they are used to update configuration data in an automated fashion. Monthly vulnerability scans for application servers and semiannual scans for CBIS database servers are performed where physical verifications are applied and any deviations are corrected. Without this baseline configuration, the execution of vulnerability scans for anomalies would be unattainable for OPM's CIO review of the integrity of configuration data.

The alternative analysis regarding the transition from CIS to DISA as a standard configuration in the FAA ESC data center have been documented. The implementation schedule transitioning from CIS to DISA is expected to be completed in Q1 of FY2020. CBIS continues to remain under the CIS configuration until production deployment of DISA.

Recommendation 3: We recommend that the CBIS application meet the requirements of OMB M-11-11 by requiring multi-factor authentication using PIV credentials.

Management Response: We concur. We recognize that CBIS is unable to comply with Homeland Security Presidential Directive 12 (HSPD-12) that calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the employees of federal contractors. In May 2019, OCFO developed a feasibility study to examine the possibility of implementing this security requirement. CBIS is currently preparing to enter the migration implementation stage for transitioning to FAA's ESC's shared service financial management platform. CBIS sponsor and stakeholders approved the business functional and technical requirements, and feasibility study reports performed in accordance of GSA, Unified Shared Service Management's Modernization and Migration Management Playbook (MP3) Engagement/Discovery stages. As a part of the implementation stage in its migration to the FAA ESC's Delphi solution, OPM plans to incorporate the requirements of the HSPD-12 directive. This represents OCFO's course of action to adhere to security standards under OMB 11-11 and HSPD-12.

Recommendation 4: We recommend that OPM ensures system admins receive incident response training for CBIS.

Management Response: We partially concur with the intent of the underlying finding, however we do not agree with the portion that pertains to IR-02 as it is an Agency Common Security Control which CBIS inherits from OPM. Incident Response (IR) training is covered in the annual Security Awareness Training which is completed by all CBIS personnel included system administrators. In addition, CBIS Financial Operations Management (FOM) conducts IR training as part of their annual

Disaster Recovery Exercise in conjunction with ESC-EDC FAA personnel.

We are aware the IR training should be a part of all system admin specialized training and will work with OCFO to ensure additional IR training is being performed outside of the Annual Security Awareness Training.

Recommendation 5: We recommend that OPM maintain an approved risk acceptance for the unsupported software until the system is transitioned to a supported platform.

Management Response: We concur. Management accepts the risk of utilizing unsupported [redacted] software that supports OPM's procurement operations. OCFO submitted to CIO a draft Risk Acceptance Waiver which is undergoing the final review and signature process. Upon completion, CIO will provide the completed documentation to IOC.

Recommendation 6: We recommend that OPM removes or updates the unsupported software from its environment.

Management Response: We concur. We recognize that the procurement system utilizes an unsupported version [redacted] (version [redacted]). However, the [redacted] application configuration settings are only operable in the [redacted]. In May 2019, OCFO completed its Discovery stage in preparation for migrating its financial management processes to FAA's ESC Delphi solution. OPM plans to leverage the FAA ESC's upgraded technology strategy for its financial management and procurement business applications. This represents OCFO's course of action to ensure its systems (to include the procurement application) is in line with the required government defined IT architecture and technology standards.

Recommendation 7: We recommend that OCFO ensure enforcement of multi-factor authentication at the CBIS datacenter for non-console access.

Management Response: We partially concur as acknowledged in recommendation #3 that the CBIS application does not enforce PIV authentication at the application level where credit card information would be stored. OCFO's course of action to adhere to security standards under OMB 11-11 and HSPD-12, is by transitioning CBIS to the FAA ESC Delphi financial management solution.

However, OPM does not believe a weakness exists with the procedures to authenticate access to the ESC data center. FIPS199 impact levels designates CBIS as a moderate system for confidentially, integrity and availability. Under the NIST SP 800-53 statute (PE-2 Physical Access Authorizations control), a moderate system is not required for multifactor authentication for physical access. In compliance with FISMA and DOT/FAA regulations, ESC-EDC deploys NIST SP 800-53 physical security controls.

The observation reference Payment Card Industry Data Security Standards (PCI DSS), which is an information security standard for organizations that handle branded credit cards from the major card schemes, does not relate to NIST regulations regarding to 'non=console access into the data

environment'.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Rochelle Bayard, Associate Chief Financial Officer, 202-606-4366, and Rochelle.Bayard@opm.gov.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100