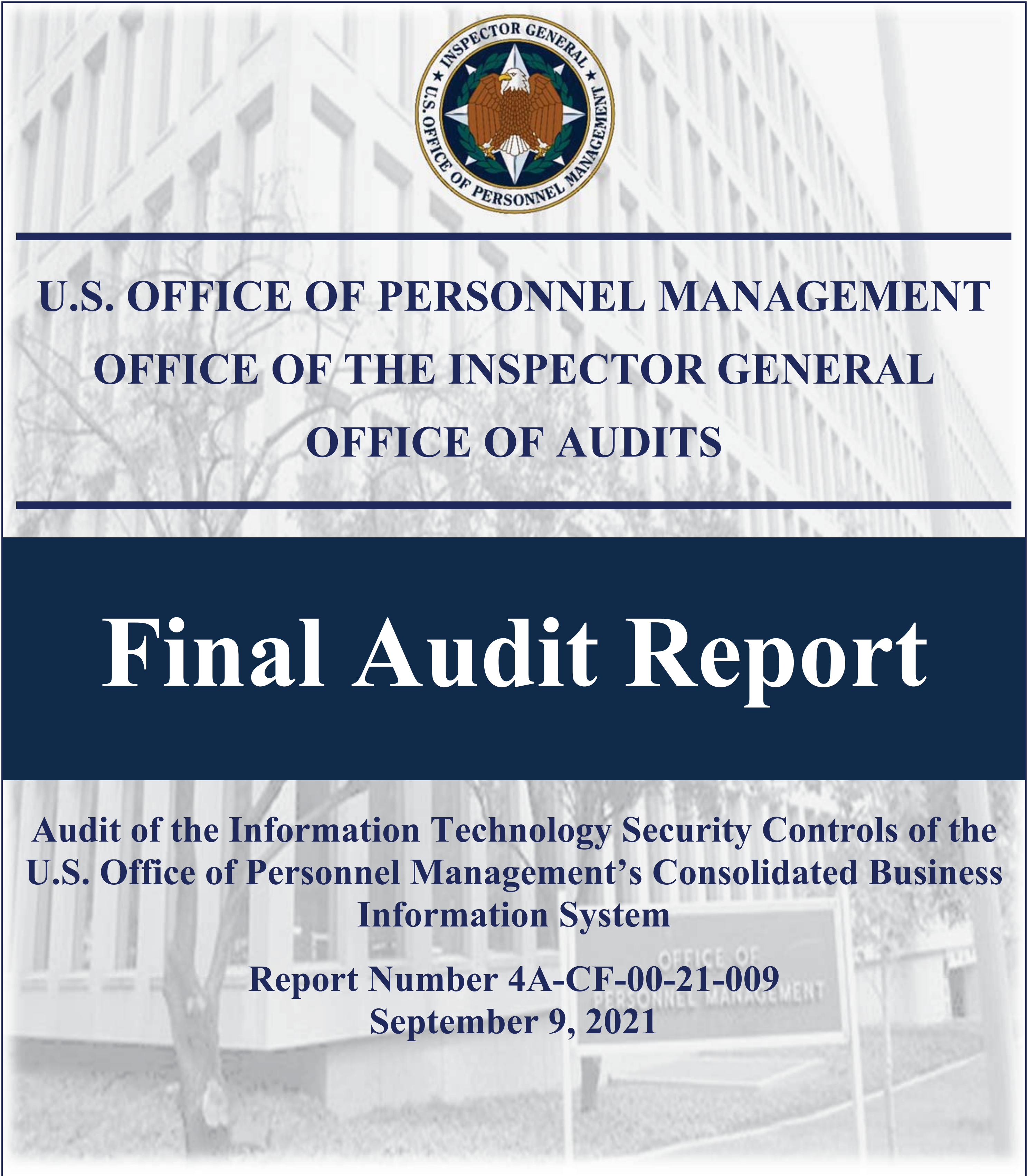

U.S. OFFICE OF PERSONNEL MANAGEMENT

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-00-21-009
September 9, 2021

# 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-00-21-009** **September 9, 2021**

### 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 perform audits of IT security controls of agency systems.

### What Did We Audit?

We 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 on April 5, 2021. The Authorization was granted for up to 90 days.
- The CBIS security categorization is consistent with Federal Information Processing Standards 199 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.
- The Office of the Chief Financial Officer did not perform a security assessment but has identified the deficiency.
- Continuous Monitoring for CBIS was conducted in accordance with OPM's quarterly schedule for fiscal year 2020.
- The CBIS contingency plan was completed in accordance with NIST Special Publication (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** |
| **DATA Act** | **Digital Accountability and Transparency Act of 2014** |
| **FAA-ESC** | **Federal Aviation Administration Enterprise Security Center** |
| **FIPS** | **Federal Information Processing Standards** |
| **FISMA** | **Federal Information Security Modernization Act** |
| **IT** | **Information Technology** |
| **NIST SP** | **National Institute of Standards and Technology's Special Publication** |
| **OCFO** | **Office of the Chief Financial Officer** |
| **OCIO** | **Office of the Chief Information Officer** |
| **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** |
| **SSP** | **System Security Plan** |

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# I. BACKGROUND

On December 17, 2002, the President signed into law the E-Government Act (P.L. 107 347), which includes Title III, the Federal Information Security Management Act. It requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of Inspector General evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior Act.

On May 9, 2014, the President signed into law the Digital Accountability and Transparency Act of 2014 (DATA Act) (P.L. 113-101) which includes Section 6, Accountability for Federal Funding. It requires Inspector Generals 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 publicly 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 are conducting 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, FISMA and the DATA Act require that the Office of the Inspector General perform an audit of IT security controls of this system.

This was our fourth audit of the IT security controls for CBIS. The previous audits resulted in findings and recommendations documented in Report Nos. 4A-CI-00-11-015, 4A-CF-00-17-043 and 4A-CF-00-19-026, dated June 1, 2011, September 29, 2017, and October 3, 2019, respectively. As part of this audit, we reviewed the status of open recommendations.

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 IT security controls of CBIS. The CBIS application resides in an FAA datacenter and inherits Trusted Internet Connection, networking, and platform level controls from the FAA hosting provider. We discussed the results of our audit with the OCIO and the 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;
- 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 May 2021.

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 FAA 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.

In conducting our audit, we relied to varying degrees on computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

As part of this audit, we tested a judgmental sample of NIST SP 800-53, Revision 4, controls. We chose a sample of 76 controls from a universe of 263 "moderate" controls. The sample included at least one control from each NIST control family. The judgmental sample was drawn from applicable controls that were identified in the latest security control assessment as "in place" and "system-specific." The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

Our assessment of the security controls protecting the confidentiality, integrity, and availability of CBIS are 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 CBIS internal controls taken as a whole.

The criteria used in conducting this audit included:

- 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; and

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

## 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.

Over the course of the audit, CBIS received three separate 90-day Authorization letters. The OCFO leveraged shortened Authorizations due to the efforts to migrate CBIS operations to the Federal Aviation Administration's Enterprise Service Center (FAA-ESC). The OCFO met their estimated completion date for the transition by migrating in May 2021. The most recent 90-day Authorization was signed April 5, 2021.

**The OCFO met their estimated completion date for the transition by migrating in May 2021.**

Nothing came to our attention to indicate that the CBIS authorization letters were 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 CBIS security categorization is a draft document that has not been signed by the Chief Information Security

Officer, Chief Privacy Officer, nor the Authorizing Official. However, there is an open POA&M requiring the security categorization to be signed.

The security categorization of CBIS appears to be consistent with FIPS 199 and NIST SP 800-60, Revision 1, requirements, and we agree with the categorization of "moderate."

The lack of an approved security categorization document would normally result in an audit finding. However, since there is an open POA&M for this specific issue, we will forgo issuing a recommendation.

## 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 the OPM's Office of Privacy and Information Management in January 2021. 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 December 2020, at the time of the Authorization.

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

## 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;
- Authorizing Official;
- System Owner;
- Other Designated Contacts;

- Assignment of Security Responsibility;
- System Operational Status;
- General Description/Purpose;
- Information System Type;
- System Environment;
- System Interconnection/Information Sharing;
- System Categorization;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the current CBIS SSP, last updated in November 2020, and determined that it adequately reflects the system's current state. Nothing came to our attention to indicate that the CBIS system security plan 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. A Risk Assessment Report assesses the risk to the system for each weakness identified during the security controls assessment.

**The most recent independent assessment was conducted in May 2017.**

The CBIS Security Assessment Plan and Risk Assessment Report were created by the OCIO Information System Security Officer in March 2017 and September 2020, respectively. The most recent independent assessment was conducted for the Authorization in May 2017. The OCFO did not perform a follow-up risk assessment on the system due to plans to migrate to FAA-ESC. The OCFO has an existing POA&M to perform a security assessment. The Authorization letter details the deficiencies related to the assessment and the system received a shortened ATO to address the issues.

Nothing came to our attention to indicate that the CBIS Security Assessment Plan or 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 2020 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, approved in November 2020, 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 July 2020. The test consisted of a failover to the disaster recovery environment for technical verification and to test server recovery capabilities. The functional test was considered successful although there were issues with network connectivity to the disaster recovery site. All lessons learned were documented to improve contingency planning activities moving forward.

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

## H. PLAN OF ACTION AND MILESTONES

A 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.

**The CBIS POA&Ms are 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 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;
- Media Protection;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection;

- 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. OPM's response to open recommendations from the prior audit report can be found under each control weakness identified.

### 1) Control CM-6 – Configuration Settings

There are not any documented configuration settings for the Exadata Oracle Linux operating system in use by the CBIS.

The FAA-ESC manages the operating system baseline configurations. FAA has documented Defense Information Systems Agency Security Technical Implementation Guide standards for only two of the three operating systems that support CBIS.

NIST SP 800-53, Revision 4, states 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 operational requirements … ."

Failure to document standard security configuration settings increases the risk that servers are not configured appropriately. If misconfigurations are left undetected, it can create a potential gateway for unauthorized access or malicious activity.

There is an open recommendation from prior report no. 4A-CF-00-19-026 (Recommendation 2) recommending that the OCFO work with FAA to implement standard configuration settings for all operating platforms in use by CBIS.

**OPM Response:**

***"We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.***

***The new financial system of record, DELPHI, contains standard security configuration settings for all operating platforms as a part of the shared services offering."***

**OIG Response:**

We acknowledge that CBIS is in the process of being decommissioned and all lower-level environments have been removed from operations. However, there are still production systems running, albeit with limited, read-only access, that OCIO does not plan to decommission until later in fiscal year 2021. Therefore, the weaknesses identified in the prior audit report still exist while the system is online.

This recommendation will remain open until all services are offline. We recommend that the OCIO provide OPM's Internal Oversight and Compliance office with evidence that the system has been completely removed from OPM's network. This response also applies to report no. 4A-CF-00-19-026, Recommendations 3 and 4.

### 2) Control IA-2(12) – Acceptance of Personal Identity Verification (PIV) Credentials

CBIS does not enforce multi-factor authentication using Personal Identity Verification (PIV) credentials. Users log in via username and password.

OPM does not have an existing POA&M for this finding. OPM is currently in the migration stage of transitioning to the FAA-ESC Delphi solution based on the Office of Shared Solutions and Performance Improvement M3 Playbook guidance.

**CBIS does not enforce multi-factor authentication using PIV credentials.**

OMB M-11-11 requires all Federal information systems to use PIV credentials for multi-factor authentication.

By not enforcing multi-factor authentication using PIV credentials, OPM is at an increased risk of a hacker gaining unauthorized access to data and mishandling of sensitive information.

There is an open recommendation from prior report 4A-CF-00-19-026 (Recommendation 3) recommending that the CBIS application meet the requirements of OMB M-11-11 by requiring multi-factor authentication using PIV credentials.

**OPM Response:**

***"We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021.***

***As a part of the migration, the FAA Delphi environment meets the requirements of OMB M-11-11, by authenticating users with OMB's MAX system with a PIV card. OMB's MAXAuthentication Cloud Service is now responsible for authenticating OPM users when accessing the financial and procurement applications within the shared services environments."***

3) **Control IR-02 – Incident Response Training**

We were informed that incident response training for CBIS personnel is not conducted. OPM is aware that the incident response training should be part of all system administration specialized training for CBIS.

OPM has not addressed this deficiency to ensure system administrators receive incident response training for CBIS personnel.

NIST SP 800-53, Revision 4, states, "The organization provides incident response training to information system users consistent with assigned roles and responsibilities … ."

Failure to perform incident response training increases the risk that OPM will fail to identify and report suspicious activities both from external and internal sources.

There is an open recommendation from prior report 4A-CF-00-19-026 (Recommendation 4) recommending that OPM ensure system administrators receive incident response training for CBIS.

**OPM Response:**

***"We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.***

***Moreover, OPM will confirm with FAA that incident response training is conducted for its system administrators as a part of the shared services offering."***

4) **Control SA-22 – Unsupported Software Component**

CBIS uses an unsupported version of PRISM which has not been supported by the vendor for almost seven years. CBIS operations transitioned to the FAA's Delphi environment which operates on a supported version of PRISM. Prior to the transition, OPM had performed a risk analysis and maintained a risk acceptance document for PRISM.

NIST SP 800-53, Revision 4, states that an organization "Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer … ."

Failure to upgrade system software can lead to vulnerabilities and exploits that are unable to be remediated.

There is an open recommendation from prior report 4A-CF-00-19-026 (Recommendation 6) recommending that OPM remove or update the unsupported software from its environment.

**OPM Response:**

***"We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.***

***The migration to the FAA ESC's shared service financial management platform leverages upgraded technology for the financial management and procurement business applications. OPM is now using the FAA ESC PRISM, which is on version 7.4 and supported by the vendor, Unison. Access to the unsupported software in CBIS has been removed and the decommissioning process for the environment has begun as of June 2021."***

**OIG Response:**

In response to the draft audit report, the OCFO provided evidence detailing an emergency request to decommission the legacy OPM PRISM solution. The OCFO has since shut down the CBIS program that used the unsupported version of PRISM, remediating Recommendation 6 from the 2019 audit. We support closure of the recommendation.

## J. PRIOR AUDIT RECOMMENDATIONS

As part of this audit, we reviewed prior audit reports to follow-up on open recommendations from those reports. The sections below represent recommendations that OCFO was able to implement during fieldwork.

### 1) Control AT-3 – Role-Based Security Training

During the fiscal year 2019 CBIS audit, we identified a control weakness pertaining to role-based security training for CBIS personnel. OPM requires all employees and contractors to complete annual security and privacy awareness training as well as role-based security training tailored to the individual's assigned IT roles and responsibilities. At that time, CBIS personnel were not performing role-based specialized training.

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."

OPM provided annual training records of FAA personnel in response to our information request. The evidence is sufficient, and we support closure of the prior audit 4A-CF-00-19-026 Recommendation 1.

2) **Control SA-22 – Risk Acceptance**

The fiscal year 2019 audit identified that CBIS used an unsupported software which is highly vulnerable. CBIS cannot operate without this software, which has not received security updates for almost nine years. OPM is in the process of transitioning to a DELPHI solution which is supported by the vendor. However, they still have the old systems online as they are performing a phased transition. OPM must maintain an approved risk acceptance for the unsupported software until the transition has been completed.

During the prior audit, we referenced a risk acceptance document that had not been approved. The OCFO has since approved the risk acceptance. Therefore, we support closure of the prior audit 4A-CF-00-19-026 Recommendation 5.

3) **Multi-Factor Authentication to Datacenter**

During the site visit to the CBIS primary datacenter in June 2019, we identified a weakness in physical access controls. Access to the datacenter did not require multi-factor authentication. We recommended that the OCFO ensure enforcement of multi-factor authentication at the CBIS datacenter for direct server access.

The OCFO and FAA stated that they have improved physical access controls by installing a turnstile at the datacenter entrance requiring a badge and personal identification number. This satisfies the recommendation, and we support closure of the prior audit 4A-CF-00-19-026 Recommendation 7.

# APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Financial
Officer

June 22, 2021

MEMORANDUM FOR CHIEF, INFORMATION SYSTEMS AUDITS GROUP
ERIC W. KEEHAN

FROM: MARGARET P. PEARSON
Acting Chief Financial Officer

GUY V. CAVALLO
Acting Chief Information Officer

SUBJECT: Office of Personnel Management Response to the Office of the Inspector General Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Consolidated Business Information System Report No. 41-CF-00-21-009

Thank you for providing the Office of Personnel Management (OPM) the opportunity to respondto the Office of the Inspector General (OIG) draft report, *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Consolidated Business Information System*, Report No. 4A-CF-00-21-009, dated June 4, 2021.

In June 2021, OPM began decommissioning CBIS and anticipates that all applications will be fully decommissioned by the end of the fiscal year. For this reason, OPM notes that any recommendations not fully implemented will soon be obsolete.

Responses to your recommendations, all of which have been rolled forward from previous reports issued by the OIG, including planned corrective actions, as appropriate, are providedbelow.

**Recommendation 1 (Rolled-over from 4A-CF-00-21-009, rec #2):** We recommend thatthe OCFO work with FAA to implement standard security configuration settings for all operating platforms in use by CBIS.

***Management Response:*** *We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.*

*The new financial system of record, DELPHI, contains standard security configuration settings for all operating platforms as a part of the shared services offering.*

**Recommendation 2 (Rolled-over from 4A-CF-00-21-009, rec #3):** We recommend thatthe CBIS application meet the requirements of OMB M-11-11 by requiring multi-factor authentication using PIV credentials.

***Management Response:*** *We concur, however, CBIS is in the process of being decommissioned , and all lower level environments have been removed from operations.CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021.*

*As a part of the migration, the FAA Delphi environment meets the requirements of OMB M-11-11, by authenticating users with OMB's MAX system with a PIV card. OMB's MAXAuthentication Cloud Service is now responsible for authenticating OPM users when accessing the financial and procurement applications within the shared services environments.*

**Recommendation 3 (Rolled-over from 4A-CF-00-21-009, rec #4):** We recommend thatOPM ensure system administrators receive incident response training for CBIS.

***Management Response:*** *We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.*

*Moreover, OPM will confirm with FAA that incident response training is conducted for its system administrators as a part of the shared services offering.*

**Recommendation 4 (Rolled-over from 4A-CF-00-21-009, rec #6):** We recommend thatOPM remove or update the unsupported software from its environment.

***Management Response:*** *We concur, however, CBIS is in the process of being decommissioned, and all lower level environments have been removed from operations. CBIS is not currently the OPM core financial system of record as we migrated to using FAA's shared services in May 2021. We recommend that this recommendation be closed.*

*The migration to the FAA ESC's shared service financial management platform leverages upgraded technology for the financial management and procurement* *businessapplications. OPM is now using the FAA ESC PRISM, which is on version 7.4 and supported by the vendor, Unison. Access to the unsupported software in CBIS has been removed and the decommissioning process for the environment has begun as of June 2021.*

We appreciate the opportunity to respond to this draft report. If you have any questions regardingour response, please contact or CFO point of contact Erick Borda at (202) 606-2413, or the CIO contact Darrin McConnell at (202) 606-6210, Darrin.McConnell@opm.gov.

Cc:
Janet Barnes
Rochelle Bayard
Erick Borda
Cord Chase
Darrin McConnell

# 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