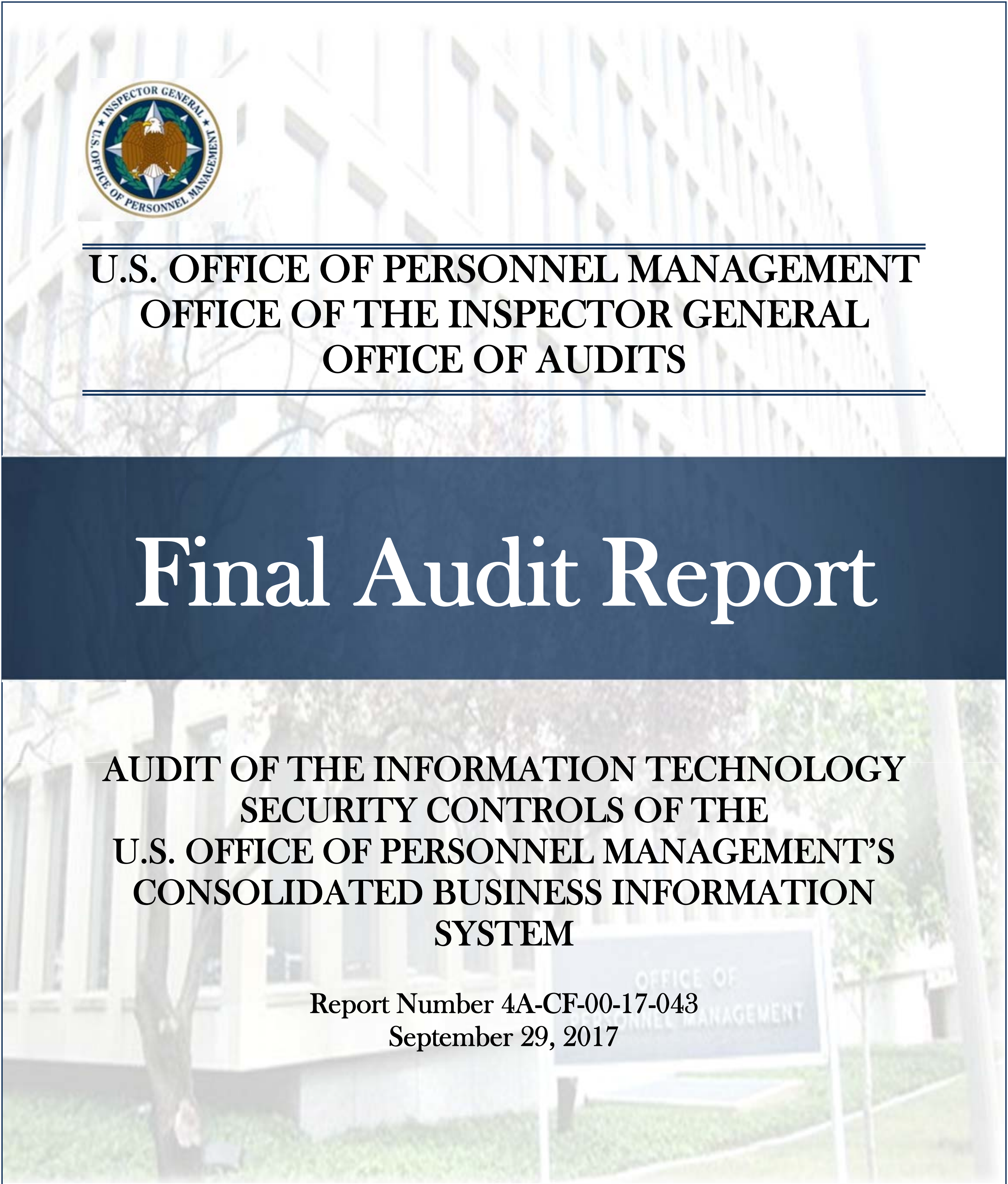

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

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-00-17-043
September 29, 2017

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-00-17-043 **September 29, 2017**

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 an audit of IT security controls of this system.

What Did We Audit?

The OIG has 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 Security 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 of CBIS was completed in 2017. An authorization to operate was granted for up to three years.
- The security categorization of CBIS is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the categorization of "moderate."
- OPM has completed a Privacy Impact Assessment for CBIS.
- The CBIS System Security Plan generally follows the OCIO template, but there were instances where the documentation was incomplete.
- An independent security controls assessment has been performed for CBIS, but elements of the test work were missing and/or incomplete and not all of the identified control weaknesses were included in the CBIS risk assessment.
- CBIS has been subject to routine testing as part of OPM continuous monitoring.
- A contingency plan was developed for CBIS that is generally in compliance with NIST SP 800-34 Revision 1 and OCIO guidance.
- The CBIS Plan of Action and Milestones (POA&M) documentation did not include all required information and known weaknesses, and did not accurately reflect targeted weakness remediation deadlines.
- We evaluated a subset of the system controls outlined in NIST SP 800-53 Revision 4. We determined most of security controls tested appear to be in compliance, however we did note one area for improvement.

ABBREVIATIONS

ATO	**Authorization to Operate**
CBIS	**Consolidated Business Information System**
DATA Act	**Digital Accountability and Transparency Act**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Management Act**
GAO	**U.S. Government Accountability Office**
ISCMP	**Information Security Continuous Monitoring Plan**
IT	**Information Technology**
IG	**Inspector General**
MRB	**Management Review Board**
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**
POA&M	**Plan of Action and Milestones**
PIA	**Privacy Impact Analysis**
PTA	**Privacy Threshold Analysis**
Authorization	**Security Assessment and Authorization**
SAR	**Security Assessment Report**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

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. It 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) the results of IG 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. As part of our evaluation, we will review the Office of Personnel Management's (OPM) FISMA compliance strategy and document the status of their compliance efforts.

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 the Office of the Inspector General (OIG) to (1) conduct a review of 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 are conducting an evaluation of 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 OIG perform an audit of IT security controls of this system.

OPM recently moved the CBIS technical infrastructure to a new technical environment – a shared service provider managed by another government agency.

OPM's Office of the Chief Information Officer (OCIO) and OCFO, in conjunction with the external shared service provider, share responsibility for implementing and managing the IT security controls of CBIS. 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 goal was to perform an evaluation of the security controls for CBIS to ensure that the OCIO and the OCFO officials have managed the implementation of 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 carried out by reviewing the degree to which a variety of security program elements have been implemented for CBIS, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- Privacy Impact Assessment (PIA);
- 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

This performance audit was conducted 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 2017.

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 OCIO and OCFO program offices with CBIS security responsibilities, 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 "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 internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- 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;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- The Federal Information System Controls Audit Manual;
- 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, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to 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, Guide for Mapping Types of Information and Information Systems to Security Categories;

- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;

- FIPS 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 the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with the 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 May through August 2017 in 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 attesting that a system's security controls meet security requirements 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 fully mature program in place to continuously monitor system security controls, therefore a current Authorization is required for every OPM system.

CBIS was most recently authorized to operate (ATO) on May 1, 2017. This ATO is valid for up to three years and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

CBIS has a current Authorization, valid for up to three years.

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 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 Publication 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 Publication 199 and NIST SP 800-60 requirements, and we agree with the categorization of "moderate."

C. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis (PTA) screening of federal information systems to determine if a PIA is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system.

A PTA was not included in the CBIS Authorization package. However, a PIA was completed and approved by OPM's Chief Privacy Officer in April 2017.

A privacy impact assessment was performed for CBIS.

We did not detect any issues with the CBIS PIA.

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 an SSP for each system, and provides guidance for doing so.

The SSP for CBIS was developed using the OCIO's SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires that the following elements be documented within the SSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Laws, Regulations, and Policies Affecting the System;
- System Environment;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- System Interconnection/Information Sharing;
- General Description/Purpose;

- Other Designated Contacts;
- Completion and Approval Dates.
- Security Control Selection;
- Minimum Security Controls; and

The current SSP was signed on April 7, 2017. However, the CBIS SSP does not adequately address all of the requirements of NIST. Specifically, we found instances of the following issues:

The CBIS SSP does not contain all information required by NIST.

- Security controls that were labeled as "inherited" from another system, but the SSP did not identify which system provided the control (e.g., a general support system); and

- Controls that had previously been defined as deficient were not mapped to existing Plan of Action and Milestones (POA&M) entries.

NIST SP 800-18, Revision 1, states "it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system."

The lack of current and complete documentation about a system's security controls increases the risk that controls are not implemented and functioning as required. This increases the difficulty of assessing risks to the system and to OPM as a whole.

Recommendation 1

We recommend that OPM update the CBIS SSP in accordance with the agency's policies and NIST standards.

OPM Response:

"OPM does not concur with the recommendation. The SSP is a living document, which is updated on an ongoing basis. The SSP for the major system was updated within the timeframe required by OPM policy. Additional updates will always be expected of a living document to enhance security control descriptions, add references to newly-identified POA&Ms, or improve any other facet of the document. OPM will continue to update its security plans based on the evolution of its systems and timeframes established in OPM policy."

OIG Comment:

While we acknowledge that an SSP is a living document and is always subject to change, that does not justify the fact that critical information was simply missing from the CBIS SSP at the time the Authorizing official made the risk-based decision to authorize the system to operate. CBIS inherits security controls from multiple sources, and details about these controls should be clearly identified within the SSP for both testing and remediation purposes. We continue to recommend that OPM update the CBIS SSP in accordance with the agency's policies and NIST standards to ensure all required information is included.

E. SECURITY ASSESSMENT PLAN AND REPORT

A Security Assessment Plan and Security Assessment Report (SAR) were completed for CBIS in March and May 2017, respectively, as a part of the system's Authorization process. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization. The following issues were identified:

1) Incomplete Testing

Three elements of the CBIS security control testing process were missing and/or incomplete.

First, the assessors performing the test work noted that there were time constraints while testing 34 access controls, and that testing was not completed at the application level.

Second, there were 16 security controls applicable to CBIS that did not have any test work or results documented.

Third, the entire CBIS system environment was not accessible to the assessors at the time of testing. The CBIS system boundary includes several different logical environments (e.g., [redacted], etc.). Two of these environments had not been created at the time of the assessment testing, and therefore have not been subject to a security controls assessment.

Excluding system components and required security controls from testing increases the risk that unidentified weaknesses exist in the system. NIST SP 800-37, Revision 1, requires that organizations "Assess the security controls in accordance with the assessment procedures defined in the security assessment plan." OPM policy also requires that "All controls selected by the system (Task 2-2) are assessed."

Recommendation 2

We recommend that OPM test the CBIS security controls that were not assessed during the Authorization process.

OPM Response:

"OPM partially concurs with the recommendation. The majority of the 16 controls referred by the OIG in the draft audit report are common, management controls identified as inherited in the SSP for the major system. Therefore, these controls do not require assessment, as that would be a duplication of previous work performed. OPM concurs that additional testing is necessary for the major system's application access controls and four other controls and enhancements.

Additionally, all environments of the major system that were available at the time were assessed. The authorization to operate the system states that it is issued for the existing operating environment. As further environments are stood up, the security controls for those environments may be evaluated through OPM's continuous monitoring program."

OIG Comment:

Although a majority of the 16 controls in question are inherited from an external entity, it is critical that information about these controls (i.e., validation that they have been implemented and tested) be documented in the CBIS Authorization package so that the authorizing official can make a fully informed decision in authorizing the system to operate.

We continue to recommend that OPM ensure that all of the required security controls for all CBIS environments are tested.

2) Risk Assessment

The assessment results table showed that 89 of the 238 tested controls were not fully satisfied. Of these 89 controls, 29 were not incorporated into the CBIS risk assessment, and therefore the risk assessment was completed without a comprehensive picture of the system's potential security vulnerabilities.

Not all of the identified control weaknesses were assessed for risk.

OPM's policy requires that each weakness identified in the security controls assessment be assessed for risk as a part of the SAR.

Failure to assess the risk associated with all identified weaknesses increases the possibility that weaknesses are not properly prioritized for remediation and compound risks may not be identified.

Recommendation 3

We recommend that OPM perform an analysis to assess the risk of the 29 control deficiencies that were omitted from the CBIS risk assessment. OPM should update the CBIS risk assessment and POA&Ms to include all identified weaknesses and their risk levels.

OPM Response:

"OPM does not concur with the recommendation. All control deficiencies identified from the assessment were included in the risk assessment and added to the Security Assessment Report (SAR). The SAR included all identified risk, both residual risk inherited from the infrastructure and risk specific to the major system. POA&Ms already existed for the infrastructure system risks and new POA&Ms were created for the newly identified risks for the major system."

OIG Comment:

OPM's statement in its response to the draft audit report is inaccurate. The Risk Assessment Table does not address 29 controls that were determined to be not fully satisfied. Despite multiple opportunities for the agency to provide evidence that these controls were assessed for risk, the information has not been provided to the OIG.

F. CONTINUOUS MONITORING

OPM requires that the IT security controls of each application be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan (ISCMP) that includes a template outlining the security controls that must be tested for all information systems. This template must be tailored to each individual system's specific security control needs. All system owners are required to customize their system's ISCMP and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO routinely for centralized tracking.

We reviewed and had no issues with the two most recent continuous monitoring submissions for CBIS.

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 routinely reviewed, tested, and updated.

1) Contingency Plan

An updated contingency plan has been approved for CBIS.

The CBIS contingency plan documents the functions, operations, and resources necessary to restore and resume CBIS when unexpected events or disasters occur. The CBIS contingency plan adequately follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans. The version of the CBIS contingency plan that was approved during the Authorization process did not contain all of the required information. The contingency plan has been updated to include the missing information, but evidence that the updated version had been formally reviewed and approved was not provided to the OIG by the time we issued our draft audit report.

Failure to review and approve a contingency plan increases the risk that the document contains incomplete and/or inaccurate information.

Recommendation 4

We recommend that OPM formally review and approve the revised CBIS contingency plan.

OPM Response:

"OPM does not concur with the recommendation. Before receipt of the draft report, OPM reviewed and approved a complete contingency plan for the major system. The contingency plan was included in the authorization package that was approved by the authorizing official."

<u>OIG Comment:</u>

In response to the draft audit report, we were provided a copy of the approved contingency plan. No further action is required.

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans be tested <u>routinely</u> to determine 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 was most recently tested in August 2016. The test was identified as a tabletop test.

Nothing came to our attention to indicate that the CBIS contingency plan testing process is not adequate.

H. 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 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.

1) Incomplete POA&M Documentation

The POA&M documentation contained in the CBIS Authorization package does not follow OPM's template and does not include all of the required information (e.g., weakness IDs and affected controls).

Incomplete POA&M documentation increases the risk that weaknesses are not resolved appropriately and/or timely.

<u>Recommendation 5</u>

We recommend that OPM update the CBIS POA&M to include the information required per OPM policy.

<u>OPM Response:</u>

"After receipt of the draft report, OPM added the major system's POA&M to the new repository and added the missing data element. OPM believes this addresses the intent of the OIG recommendation and requests the item be closed."

<u>OIG Comment:</u>

In response to the draft report OCIO provided evidence that the POA&Ms had been updated. No further action is required.

2) Overdue POA&Ms

CBIS has 40 open POA&Ms dating back to 2012. While 1 POA&M is pending closure, 39 have scheduled completion dates that are over 6 months overdue. These POA&Ms should be updated to reflect any milestone changes and new reasonable estimated completion dates. If the recent move of CBIS made any of these items no longer applicable, they should be removed from the CBIS POA&M.

OPM's policy states that "Should expected completion dates for milestones of POA&Ms be missed, the associated POA&Ms will be brought before the [Management Review Board (MRB)] for review in order to address any corrective actions needed for remediating the POA&Ms in accordance with the requirements defined in the Authorization to Operate (ATO) issued for the applicable system. Updated milestones and expected completion dates will be required for the following MRB meeting."

Failure to properly maintain a system's POA&M increases the likelihood of weaknesses not being addressed in a timely manner and potentially exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

<u>Recommendation 6</u>

We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items and close any that are no longer applicable. This action plan should include realistic estimated completion dates.

OPM Response:

"OPM partially concurs with the recommendation. During the course of the audit, OPM provided the OIG the POA&M for the weaknesses identified during the assessment and authorization of the system. The items on the POA&M included the action plan, with estimated completion dates, for the remediation of the weaknesses."

As discussed in the prior recommendation, the POA&M for the major system had not yet transitioned to the new repository during the course of the audit. After receipt of the draft report, OPM updated the POA&M items with new estimated completion dates, taking into consideration any factors that have led to the previously missed dates. All POA&Ms that were no longer relevant have been remedied within the confines of our POA&M repository system of record. OPM believes this addresses the intent of the OIG recommendation and requests the item be closed."

OIG Comment:

As part of the audit resolution process, we recommend the OCIO provide OPM's Internal Oversight and Compliance division with evidence that this recommendation has been implemented.

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 a subset of these controls had been implemented for CBIS. We tested approximately 20 controls from NIST SP 800-53, Revision 4, including one or more controls from each of the following control families:

- Access Control;
- Security Assessment and Authorization;
- Contingency Planning;
- Incident Response;
- Planning;
- Risk Assessment;
- Audit and Accountability;
- Configuration Management;

- Identity and Authentication;
- Media Protection; and
- System and Information Integrity;
- System and Communications Protection.

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.

We determined that the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements with the following exception:

1) Control SI-4 Information System Monitoring

Monitoring a system reduces the time required to detect and mitigate attacks against an information system.

Despite the SSP reporting the use of a security tool to monitor CBIS for attacks or inappropriate access, the OCFO and/or the OCIO have not provided evidence indicating that the control is in place. Therefore, this report assumes that the control has not yet been implemented. Intrusion detection systems, log analyzers, or system event and incident management tools are some of the controls that could be used to monitor information systems.

NIST SP 800-53, Revision 4, requires that an "organization:

a. Monitor the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [organization-defined objectives]; and
   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the information [with organization-defined techniques and methods];

c. Deploy monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; and

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion . . . . "

Failure to monitor a system for attacks and unauthorized access increases the risks that an attacker can access the system undetected and then steal, delete, or corrupt the system's data.

Recommendation 7

We recommend that OPM implement tools and procedures to monitor CBIS according to NIST guidance.

OPM Response:

"OPM does not concur with the recommendation. OPM requires tools and procedures be implemented to monitor each of the systems it hosts and each of the systems that provide services to OPM. These controls are inherited from the service provider and are monitored on an ongoing basis by the OPM continuous monitoring program. OPM provided the OIG with descriptions of the services provided by the service provider, including network and security monitoring and incident response, as well as the tools that provide those services."

OIG Comment:

In response to the draft report, OCIO provided documentation indicating that CBIS inherits several NIST security controls from the external service provider. However, none of the documents provided were evidence that control SI-4 is in place. As a part of the audit resolution process we recommend that OPM provide Internal Oversight and Compliance evidence of tools and procedures implemented to monitor CBIS.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

August 18, 2017

MEMORANDUM FOR [redacted]
OFFICE OF THE INSPECTOR GENERAL

FROM: DAVID L. DEVRIES
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
CHIEF INFORMATION OFFICER

DENNIS D. COLEMAN
CHIEF FINANCIAL OFFICER

Subject: Office of Personnel Management Response to the Office of the Inspector General Audit Report No. 4A-CF-00-17-043

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report 4A-CF-00-17-043. We recognize that even the most well-run programs benefit from external evaluation and we appreciate your assessment of our operations as it will help guide our improvements to enhance the security of the data provided to OPM by the Federal workforce, the Federal agencies, Private industries, and the general public.

OPM has documented cybersecurity policies and procedures to protect OPM information and information systems, and to implement requirements in Federal law. The recommendations provided by the OIG generally state that OPM should implement its documented policies and procedures. While OPM agrees that these actions should take place, OPM does not agree with the analysis or findings supporting many of the recommendations issued by the OIG. OPM has highlighted these areas with the partially concur and not concur responses below and provided additional documentation to affirm OPM's statements and demonstrate OPM's accomplishments. We welcome a collaborative dialogue to help us fully understand the OIG's recommendations as we plan our remediation efforts so that our actions, and the closure of the recommendations, thoroughly address the underlying issues.

The response to your recommendations is provided below.

Recommendation 1
We recommend that OPM update the [major system] SSP in accordance with the agency's policies and NIST standards.

OPM Response: OPM does not concur with the recommendation. The SSP is a living document, which is updated on an ongoing basis. The SSP for the major system was updated within the timeframe required by OPM policy. Additional updates will always be expected of a living document to enhance security control descriptions, add references to newly-identified POA&Ms, or improve any other facet of the document. OPM will continue to update its security plans based on the evolution of its systems and timeframes established in OPM policy.

Recommendation 2
We recommend that OPM test the [major system] security controls that were not assessed during the authorization process.

OPM Response: OPM partially concurs with the recommendation. The majority of the 16 controls referred by the OIG in the draft audit report are common, management controls identified as inherited in the SSP for the major system. Therefore, these controls do not require assessment, as that would be a duplication of previous work performed. OPM concurs that additional testing is necessary for the major system's application access controls and four other controls and enhancements.

Additionally, all environments of the major system that were available at the time were assessed. The authorization to operate the system states that it is issued for the existing operating environment. As further environments are stood up, the security controls for those environments may be evaluated through OPM's continuous monitoring program.

Recommendation 3
We recommend that OPM perform an analysis to assess the risk of the 29 control deficiencies that were omitted from the [major system] risk assessment. OPM should update the [major system] risk assessment and POA&Ms to include all identified weaknesses and their risk levels.

OPM Response: OPM does not concur with the recommendation. All control deficiencies identified from the assessment were included in the risk assessment and added to the Security Assessment Report (SAR). The SAR included all identified risk, both residual risk inherited from the infrastructure and risk specific to the major system. POA&Ms already existed for the infrastructure system risks and new POA&Ms were created for the newly identified risks for the major system.

[A portion of the OPM response to the draft report has been removed by the OIG as it is not relevant to the Final Report.]

Recommendation [4]
We recommend that OPM formally review and approve the [major system] contingency plan.

OPM Response: OPM does not concur with the recommendation. Before receipt of the draft report, OPM reviewed and approved a complete contingency plan for the major system. The contingency plan was included in the authorization package that was approved by the authorizing official.

Recommendation [5]
We recommend that OPM update the [major system] POA&M to include the information required per OPM policy.

OPM Response: OPM partially concurs with the recommendation. OPM concurs with the OIG that the information included on the POA&M provided to the OIG during the course of the audit was incomplete;

however, the POA&M was missing only one data element required by the Office of Management and Budget and OPM policy, not the list of elements documented in the report. This missing POA&M element was first identified in a prior audit by the General Accountability Office (GAO) and OPM created an item on its POA&M to remediate the issue. Since the issuance of the GAO audit report, OPM has undergone a transition of its POA&M to a new repository that can support the inclusion of the missing data element. During the course of this OIG audit, the POA&M for the major system had not yet transitioned to use the new repository. After receipt of the draft report, OPM added the major system's POA&M to the new repository and added the missing data element. OPM believes this addresses the intent of the OIG recommendation and requests the item be closed.

Recommendation [6]
We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items and close any that are no longer applicable. This action plan should include realistic estimated completion dates.

OPM Response: OPM partially concurs with the recommendation. During the course of the audit, OPM provided the OIG the POA&M for the weaknesses identified during the assessment and authorization of the system. The items on the POA&M included the action plan, with estimated completion dates, for the remediation of the weaknesses.

As discussed in the prior recommendation, the POA&M for the major system had not yet transitioned to the new repository during the course of the audit. After receipt of the draft report, OPM updated the POA&M items with new estimated completion dates, taking into consideration any factors that have led to the previously missed dates. All POA&Ms that were no longer relevant have been remedied within the confines of our POA&M repository system of record. OPM believes this addresses the intent of the OIG recommendation and requests the item be closed.

[A portion of the OPM response to the draft report has been removed by the OIG as it is not relevant to the Final Report.]

Recommendation [7]
We recommend that OPM implement tools and procedures to monitor [the major system] according to NIST guidance.

OPM Response: OPM does not concur with the recommendation. OPM requires tools and procedures be implemented to monitor each of the systems it hosts and each of the systems that provide services to OPM. These controls are inherited from the service provider and are monitored on an ongoing basis by the OPM continuous monitoring program. OPM provided the OIG with descriptions of the services provided by the service provider, including network and security monitoring and incident response, as well as the tools that provide those services.

The audit recommendations provided in this draft report highlight that OPM and its OIG may not have a mutual understanding of OPM's work in this area. We believe further discussion regarding OIG's recommendations and findings would be beneficial in reaching resolution of the audit recommendations effectively and efficiently. Please contact us, or [redacted], if you have questions or need additional information.

cc:
[redacted]
Chief Information Security Officer

Mark W. Lambert
Associate Director, Merit Systems Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

Jason D. Simmons
Chief of Staff

Kathie Whipple
Deputy General Counsel

Jason Foster
Associate General Counsel

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