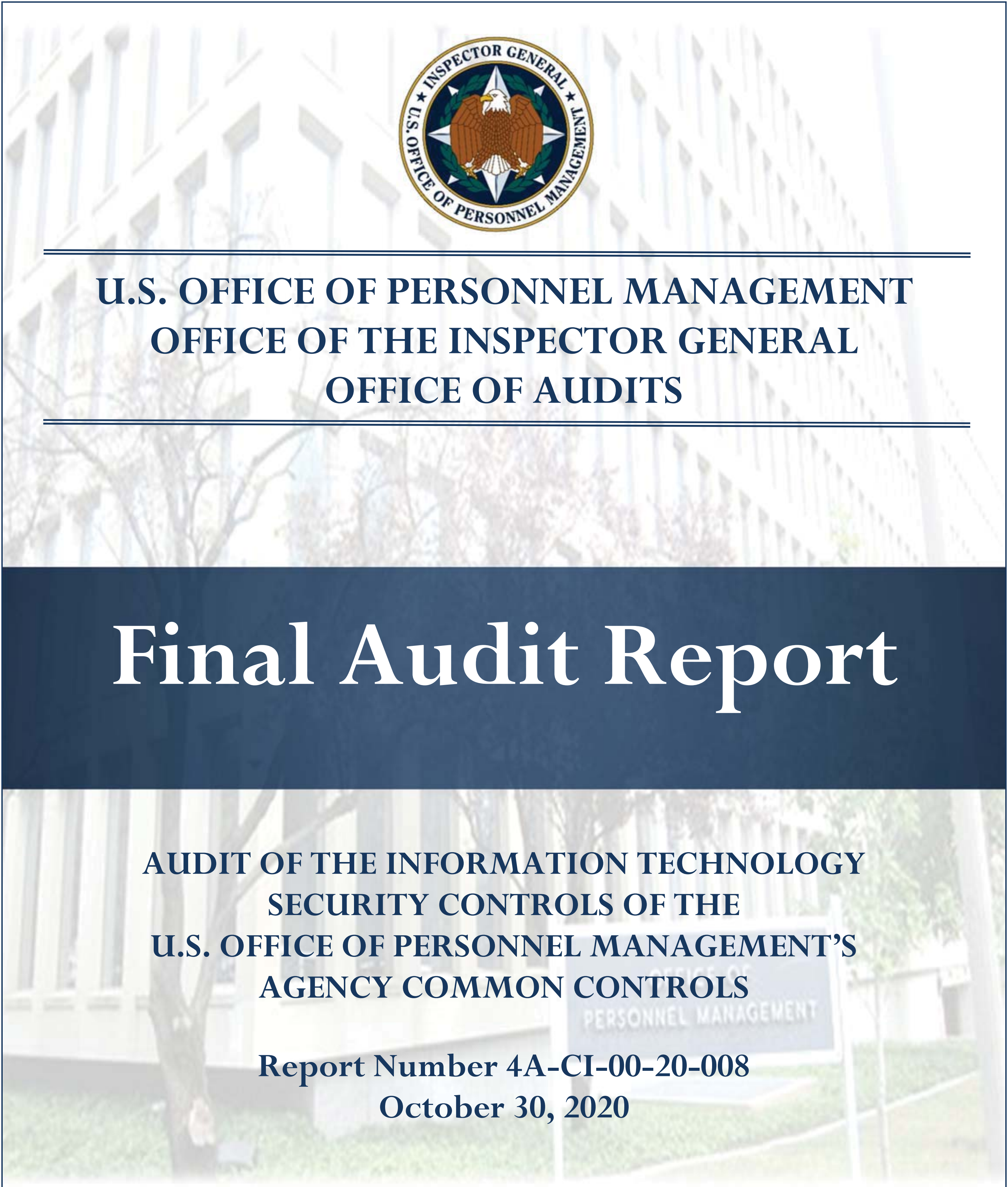

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S AGENCY COMMON CONTROLS

Report Number 4A-CI-00-20-008
October 30, 2020

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Agency Common Controls

Report No. 4A-CI-00-20-008 **October 30, 2020**

Why Did We Conduct The Audit?

The agency common controls are controls that are developed, implemented, assessed and monitored by the agency and are inherited by all of the Office of Personnel Management's (OPM) systems. The Common Security Control Collection (CSCC) lists all of the agency common controls. The Federal Information Security Modernization Act (FISMA) requires Inspectors General to complete annual evaluations of their respective agency's security programs and practices including determining the effectiveness of information security policies, procedures, and controls.

What Did We Audit?

The Office of the Inspector General completed a performance audit of the agency's common controls to ensure that the controls meet the standards established by FISMA, the National Institute of Standards and Technology, the Federal Information System Controls Audit Manual, and OPM's Office of the Chief Information Officer.

What Did We Find?

Our audit of the agency common controls listed in the CSCC determined that:

- Documentation assigning roles and responsibilities for the governance of the CSCC does not exist.
- Inconsistencies in the risk assessment and reporting of deficient controls were identified in the most recent assessment results documentation of the CSCC.
- Weaknesses identified in an assessment of the CSCC were not tracked through a plan of actions and milestones.
- Weaknesses identified in an assessment of the CSCC were not communicated to the Information System Security Officers, System Owners or Authorizing Officials of the systems that inherit the controls.
- We tested 56 of the 94 controls in the CSCC. Of the 56 controls tested, 29 were either partially satisfied or not satisfied. Satisfied controls are fully implemented controls according to the National Institute of Standards and Technology.

Michael R. Esser
Assistant Inspector General for Audits

ABBREVIATIONS

AO	Authorizing Official
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSCC	Common Security Controls Collection
FISMA	Federal Information Security Modernization Act
FSEM	Facilities, Security, and Emergency Management
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
POA&M	Plan of Action and Milestones
SAR	Security Assessment Report
SO	System Owner
SP	Special Publication

TABLE OF CONTENTS

Page

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.

The list of agency-wide common controls is documented in the Common Security Control Collection (CSCC). The CSCC contains security controls that cover the management of the security program, e.g., Office of Personnel Management (OPM) security policies or security awareness training. All systems which are owned and operated by OPM inherit the controls from the CSCC.

This was our second audit of the CSCC. The previous audit resulted in findings and recommendations documented in Report No. 4A-CI-00-13-0036, dated October 10, 2013. All four recommendations from the previous audit have been closed.

OPM's Office of the Chief Information Officer (OCIO), the Facilities, Security, and Emergency Management (FSEM) office, and OPM program offices share the responsibility for implementing and managing the controls in the CSCC. We discussed the results of our audit with OPM representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an evaluation of the agency common controls listed in the CSCC to ensure that the OCIO, FSEM and OPM program 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 accomplished by reviewing the degree to which a variety of security program elements were implemented for the CSCC, including:

- Policy and Procedures Governing the CSCC;
- CSCC Assessment Documentation; and
- CSCC Control Testing.

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 the CSCC, including the evaluation of the Information Technology (IT) security controls in place as of May 2020.

We considered the internal control structure for various OPM systems 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 staff and other OPM program officials with system security responsibilities and reviewed documentation. 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 the agency common controls listed in the CSCC 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 CSCC internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Security Authorization Guide;

- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;

- P.L. 113-283, Federal Information Security Modernization Act of 2014; and

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

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 performed the audit, as established by the Inspector General Act of 1978, as amended. We conducted the audit from November 2019 through May 2020 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 the CSCC 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. POLICY AND PROCEDURES GOVERNING THE CSCC

During the course of fieldwork interviews, representatives from OPM conveyed that the controls in the CSCC are to be independently tested in a three-year cycle; that the same Security Assessment and Authorization policy and procedures that guide individual information systems are to be used for testing CSCC controls; and that indirectly, the Chief Information Security Officer is responsible for ensuring the cybersecurity controls are tested and fully implemented.

OPM has not developed a document that assigns responsibilities for governing the CSCC.

We reviewed several documents that OPM provided pertaining to the CSCC. The Security Authorization Guide references the CSCC twice. The first reference is to provide a definition and the second is to state that the inheritance of the CSCC controls must be validated. The Use of the Common Security Controls Collection document defines the CSCC and provides instructions for Information System Security Officers (ISSOs) to determine which controls in their system are part of the CSCC and to not include those controls in a system security controls assessment. A 2013 Memorandum to System Owners (SOs) and Designated Security Officers regarding the CSCC stated that certain controls would no longer be part of the CSCC and issued a revised version of the CSCC. Upon completing our review of provided documentation, we did not observe any mention of the CSCC assessment requirements or roles and responsibilities as conveyed by OPM representatives during our fieldwork interviews.

According to the NIST SP 800-53, Revision 4, "The organization … Develops and disseminates an organization-wide information security program plan that … Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; … Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; … Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical) … ."

NIST SP 800-53, Revision 4, also states, "Common controls are subject to the same assessment and monitoring requirements as system-specific controls employed in individual organizational information systems. … Authorization results for common controls are shared with the appropriate information system owners and authorizing officials. A plan of action and milestones is developed and maintained for common controls that have been determined through independent assessments, to be less than effective. Information system owners dependent on common controls that are less than effective consider whether they are willing to accept the associated risk or if additional tailoring is required to address the weaknesses or deficiencies in the controls."

OMB Circular A-130 states that "To provide proper safeguards, agencies shall … Implement security policies issued by OMB, as well as requirements issued by the Department of Commerce, the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Office of Personnel Management (OPM). This includes applying the standards and guidelines contained in the NIST FIPS, NIST SPs (e.g., 800 series guidelines), and where appropriate and directed by OMB, NIST Interagency or Internal Reports (NISTIRs)."

The lack of documentation that formally assigns responsibilities for governing the CSCC, requires common controls to be assessed, and the communication of the assessment results could have a significant impact on the Authorizing Official's (AO's) ability to accurately assess and accept the risks of a system.

Recommendation 1

We recommend that OPM document the governance requirements of the CSCC that at a minimum contain the following elements as stated by NIST:

a) Assigns responsibilities for oversight of the CSCC;

b) Mandates the same assessment and monitoring requirements as system-specific controls in OPM information systems; and

c) Requires the communication of assessment results to SOs and ISSOs.

OPM Response:

"We do not concur. Within the OIG analysis, the OIG cites reviews of the OPM Security Authorization Guide, a 2013 memorandum, and a 2013 instructional document for using the CSCC. These documents were reviewed by the OIG for references to specific terms and content as the basis for this recommendation. The OPM memorandum and instructional document referred to in this report are not applicable to the nature of this metric.

During discussions throughout the audit process, OCIO informed the OIG that there are several places to look for references to requirements for the responsibilities of oversight of the agency's common controls, assessment requirements, including communication of results, and the continuous monitoring requirements. The material OPM referenced to the OIG included numerous policies, our enterprise Governance, Risk, and Compliance (GRC) tool,

and the Security Authorization Guide (with supporting appendices). These items are not cited in the report in regard to this metric and recommendation.

The OPM CSCC is not treated as a unique entity, with responsibilities and requirements that are different from other entities within the enterprise inventory. OCIO referenced locations within the Security Authorization Guide that demonstrated the CSCC is covered under the requirements within this guide. Specific requirements in association with security controls were identified in policies that were provided. Additionally, the implementation of these requirements (for example, the identification of responsibilities for the common controls) was demonstrated within the OPM GRC tool."

Office of Inspector General (OIG) Comment:

The OIG requested all policies and procedures governing the CSCC, and we received the documents mentioned in this report. Some of the documents that OPM mentioned in its response to the draft audit report were policies regarding individual controls within the CSCC. These policies do identify roles and responsibilities for the specific controls. However, they do not address the governance of the CSCC as a whole, to ensure that the collective controls are properly managed. The Security Authorization Guide OPM mentioned in its response identified roles and responsibilities for OPM authorized systems. Since the CSCC has not been categorized as a system nor is there any mention in OPM documentation that the CSCC will be treated as a system, the OIG cannot validate that the roles and responsibilities in these documents pertain to the CSCC. Additionally, OPM's documentation does not identify the individuals for those roles, such as identifying who is the CSCC AO or equivalent, the SO, or the ISSO and their contact information. We therefore continue to recommend that OPM document the governance requirements for the CSCC.

B. CSCC ASSESSMENT DOCUMENTATION

A security control assessment is an evaluation process that attests that a system's security controls are meeting the security requirements of that system and the results are used to update the risk assessment.

In 2017, OPM included the CSCC controls testing as part of another system's independent assessment. Although the CSCC controls were independently assessed, we identified inconsistencies in the assessment results documentation.

1. Risk Assessment

Agencies can use the results from controls assessments to conduct risk assessments. The results from risk assessments are used to help determine the severity of vulnerabilities identified in the control assessments and can guide and inform the agencies' responses to risk.

The assessment of the CSCC controls identified 33 deficient controls. The risk for the deficient controls was assessed in two separate documents. The two risk assessments contained conflicting information pertaining to the risk levels and residual risk of the controls. One of the risk assessments assessed 14 controls, 10 with a residual risk of high and 4 with a residual risk of low. The other risk assessment assessed 32 of the 33 controls, including the 14 in the other risk assessment, but excluded a Planning control. In that risk assessment, residual risk was assigned to only one control, and the other 31 residual risks were not stated.

2. Security Assessment Report

Security Assessment Reports (SARs) document assessment results to determine if the security controls are implemented correctly, operating as intended, and produce the desired outcome with respect to meeting security requirements.

The SAR also contained inconsistent information with regard to the number of controls with residual risk and the categorization of the residual risk when compared to the risk assessments. The SAR stated the residual risk for eight controls, with one categorized as moderate and seven controls as low. The total number of eight controls is inconsistent with either risk assessment document. As stated previously, one risk assessment categorized 14 controls, 10 as high and 4 as low. The other risk assessment only categorized 1 control as low and did not state a categorization of risk for the other 31 controls.

3. Plan of Action and Milestones

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.

The 33 deficient controls identified in the risk assessment were not tracked through POA&Ms nor were they communicated to the ISSOs, SOs, or AOs of the systems that inherit the controls. OPM officials stated that no POA&Ms relating to the CSCC deficiencies were listed in the official document repository. OPM officials also stated that "artifacts on the communications to ISSOs or SOs could not be found."

Since the assessment of the CSCC controls did not properly document the risk assessment of the deficient controls and POA&Ms of the deficient controls were not documented nor communicated, the AOs did not receive all of the information to properly assess the risks to their systems. Conducting a new independent assessment of the CSCC controls would provide OPM the opportunity to address the identified documentation issues and properly document the assessment. Failure to properly document an assessment can increase the likelihood that significant risks may not be properly assessed.

NIST SP 800-53, Revision 4, states, "Common controls are subject to the same assessment and monitoring requirements as system-specific controls employed in individual organizational information systems."

The OPM Security Assessment and Authorization Guide explains that "In order to perform an assessment of the security controls implemented by the system, an independent assessor must be employed to conduct the security control assessment."

Recommendation 2

We recommend that OPM conduct an independent assessment of the controls that make up the CSCC.

OPM Response:

"We concur. The OCIO recognizes the need for another independent assessment and has one planned for fiscal year 2021.

The OCIO would also like to provide clarification on the content provided in the report. During the audit, the OCIO described the activities that occurred during the last assessment of controls that was conducted. The documents that were provided were not meant to be compared in the way portrayed in the report. This evidence was intended to show that there were multiple control assessments and risk evaluations which demonstrate an evolution of the risk assessment over time. Further detail, including clarification on the number of residual risks, is outlined in technical comments."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO 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 the OCIO agrees to implement.)

The OIG requested the most recent assessment of the controls within CSCC. All of the artifacts mentioned in this section of the report were dated 2017. In both assessment results tables, the controls were tested in the same month. The two risk assessments were dated the same day. We did not observe any evidence of multiple control assessments and risk evaluations as mentioned in OPM's response to the draft audit report. The assessment report concluded that there were eight residual risks, however the assessment documentation does not demonstrate how that conclusion was made.

Recommendation 3

We recommend that OPM update the CSCC to accurately reflect the controls in place and provided to the agency's systems.

OPM Response:

"We partially concur. The OCIO has documented the control status for the enterprise common security controls and updating their current implementation status to be shared with all subscribers of those controls.

However, the OCIO does not agree that this corrective action cannot take place until the prior recommendation is complete. The OCIO understands its current state of the controls based on the assessments which were performed in accordance with its policies and procedures. While a future assessment may bring to light new information that may bring cause for additional updates to a living document, the OCIO does not agree that it should retain audit recommendations necessitating an activity be conducted in the future based on a potential outcome of another activity planned to take place in the future."

OIG Comment:

The intent of the note in the draft audit report stating that completion of this recommendation was contingent upon closure of recommendation 2 was to ensure that OPM tracks and communicates the deficient controls identified in the recommended independent assessment. We internally discussed OPM's response to this recommendation and determined that OPM has made a valid point. Implementation of this recommendation is not necessarily contingent upon the completion of recommendation 2. We removed the note from the final report.

C. CSCC CONTROLS TESTING

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 the CSCC controls had been adequately implemented. The CSCC contains 94 controls spanning the 18 control families. We used judgmental sampling to select the controls for testing and the results were not projected to the universe. We tested 56 controls as outlined in NIST SP 800-53, Revision 4, and identified 29 deficient controls, with 1 or more from each of the following 16 control families:

Control Family Name	Number of Deficient Controls
Access Control	1
Audit and Accountability	1
Awareness and Training	2
Configuration Management	1
Contingency Planning	1
Identity and Authentication	1
Incident Response	3
Media Protection	1
Personnel Security	6
Physical and Environmental Protection	5
Planning	2
Program Management	1
System and Communication Protection	1
System and Information Integrity	1
System Maintenance	1
System and Services Acquisition	1
Total	**29**

The CSCC includes 26 physical and environmental controls that are required for each of OPM's three datacenters. We tested 22 physical and environmental controls for the Theodore Roosevelt Building data center in Washington D.C. We did not test the physical and environmental controls at OPM's two other data centers in Macon, Georgia and Boyers, Pennsylvania because of time and resource constraints. Also, of the 29 total controls we identified as deficient, 18 were partially satisfied and 11 were not satisfied. Satisfied controls are fully implemented controls according to NIST.

The results of our control testing were communicated to OPM officials four times during the course of this audit and each time we gave OPM the opportunity to provide evidence that the deficient controls were in place. We received and evaluated additional evidence and updated our control testing results accordingly. The final detailed results of our control testing for the CSCC controls were provided to OPM in advance of the draft report issuance and will not be detailed in this report.

As mentioned above, the roles and responsibilities for ensuring the CSCC controls are properly implemented have not been documented. Therefore, we will not make a recommendation on each of the deficient controls as they are symptomatic of the larger underlining issue, the lack of CSCC governance documentation that we addressed with recommendation 1. However, as mentioned earlier, the 2017 CSCC assessment results were not communicated to ISSOs, SOs, or AOs whose systems inherit these controls. The CSCC contains agency common controls that are inherited by all OPM systems and are therefore not required to be tested as part of individual system security control assessments. The AOs for each system assume that the CSCC controls are tested independently and that the results are appropriately communicated to them. The AOs rely on the results of the tested controls to assess the level of risk to their systems. Failure to communicate assessment results can significantly impact the AOs ability to accurately assess the level of risks to their systems.

NIST SP 800-53, revision 4, states, "Authorization results for common controls are shared with the appropriate information system owners and authorizing officials. A plan of action and milestones is developed and maintained for common controls that have been determined through independent assessments to be less than effective. Information system owners dependent on common controls that are less than effective consider whether they are willing to accept the associated risk or if additional tailoring is required to address the weaknesses or deficiencies in the controls."

Recommendation 4

We recommend that OPM notify all Authorizing Officials of the status of the controls identified from the CSCC that are not fully implemented.

OPM Response:

"We partially concur. The OCIO agrees that we should notify all System Owners and Authorizing Officials of the status of the enterprise common controls. The OCIO intends to share results of its common controls with relevant parties through its GRC tool.

However, the OCIO does not wholly agree with the results presented for several controls represented in the table on [page 10 under CSCC Controls Testing. In reference to the sharing of results described on page 11, paragraph 1], the assessment results did not provide sufficient information as to what specific assessment methods were performed, the corresponding objects utilized, and what specific control specifications were not met. In some cases, the OCIO is unable to provide a more detailed response to the results without this additional information from the OIG. This additional information is typically issued as a part of the security control assessment results documentation required for independent system assessments, allowing OPM to gain a thorough understanding of the control assessment."

OIG Comment:

The OIG provided the names of the documents reviewed and an explanation as to why the controls were deemed insufficient in the OIG CSCC Controls Testing Results spreadsheet that was provided to the Deputy Chief Information Officer (CIO), Associate CIO, Chief Information Security Officer (CISO) and Deputy CISO prior to the issuance of the draft report. If OPM were to communicate specifically which controls require additional information, the OIG would gladly provide it.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

August 17, 2020

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

FROM: Clare A. Martorana
Chief Information Officer

CLARE MARTORANA

Digitally signed by CLARE MARTORANA
Date:2020.08.2117:25:11-04'00'

SUBJECT: Audit of the U.S. Office of Personnel Management's Agency Common Controls (Report No. 4A-CI-00-20-008)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the U.S. Office of Personnel Management's Agency Common Controls, Report No. 4A-CI-00-20-008.

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

Recommendation 1: We recommend that OPM document the governance requirements of the CSCC that at a minimum contain the following elements as stated by NIST:

a) Assigns responsibilities for oversight of the CSCC;
b) Mandates the same assessment and monitoring requirements as system-specific controls in OPM information systems; and
c) Requires the communication of assessment results with System Owners and Information Security System Officers.

Management Response: We do not concur. Within the OIG analysis, the OIG cites reviews of the OPM Security Authorization Guide, a 2013 memorandum, and a 2013 instructional document for using the CSCC. These documents were reviewed by the OIG for references to specific terms and content as the basis for this recommendation. The OPM memorandum and instructional document referred to in this report are not applicable to the nature of this metric.

During discussions throughout the audit process, OCIO informed the OIG that there are several places to look for references to requirements for the responsibilities of oversight of the agency's common controls, assessment requirements, including communication of results, and the continuous monitoring requirements. The material OPM referenced to the OIG included numerous policies, our enterprise Governance, Risk, and Compliance (GRC) tool, and the Security Authorization Guide (with supporting appendices). These items are not cited in the report in regard to this metric and recommendation.

The OPM CSCC is not treated as a unique entity, with responsibilities and requirements that are different from other entities within the enterprise inventory. OCIO referenced locations within the Security Authorization Guide that demonstrated the CSCC is covered under the requirements within this guide.
Specific requirements in association with security controls were identified in policies that were provided. Additionally, the implementation of these requirements (for example, the identification of responsibilities for the common controls) was demonstrated within the OPM GRC tool.

Recommendation 2: We recommend that OPM conduct an independent assessment of the controls that make up the CSCC.

Management Response: We concur. The OCIO recognizes the need for another independent assessment and has one planned for fiscal year 2021.

The OCIO would also like to provide clarification on the content provided in the report. During the audit, the OCIO described the activities that occurred during the last assessment of controls that was conducted. The documents that were provided were not meant to be compared in the way portrayed in the report. This evidence was intended to show that there were multiple control assessments and risk evaluations which demonstrate an evolution of the risk assessment over time. Further detail, including clarification on the number of residual risks, is outlined in technical comments.

Recommendation 3: We recommend that OPM update the CSCC to accurately reflect the controls in-place and provided to the agency's systems.

Note: The corrective action for this recommendation cannot be completed until recommendation 2 is complete.

Management Response: We partially concur. The OCIO has documented the control status for the enterprise common security controls and updating their current implementation status to be shared with all subscribers of those controls.

However, the OCIO does not agree that this corrective action cannot take place until the prior recommendation is complete. The OCIO understands its current state of the controls based on the assessments which were performed in accordance with its policies and procedures. While a future assessment may bring to light new information that may bring cause for additional updates to a living document, the OCIO does not agree that it should retain audit recommendations necessitating an activity be conducted in the future based on a potential outcome of another activity planned to take place in the future.

Recommendation 4: We recommend that OPM notify all Authorizing Officials of the status of the controls identified from the CSCC not to be fully implemented.

Management Response: We partially concur. The OCIO agrees that we should notify all System Owners and Authorizing Officials of the status of the enterprise common controls. . The OCIO intends to share results of its common controls with relevant parties through its GRC tool.

However, the OCIO does not wholly agree with the results presented for several controls represented in the table on page 8 under CSCC Controls Testing. In reference to the sharing of results described on page 8, paragraph 2, the assessment results did not provide sufficient information as to what specific assessment methods were performed, the corresponding objects utilized, and what specific control specifications were not met. In some cases, the OCIO is unable to provide a more detailed response to the results without this additional information from the OIG. This additional information is typically issued as a part of the security control assessment results documentation required for independent system assessments, allowing OPM to gain a thorough understanding of the control assessment

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [redacted] [redacted], and [redacted]@opm.gov.

Technical Comments on Audit of the U.S. Office of Personnel Management's Agency Common Controls, Report No. 4A-CI-00-20-008, dated July 16, 2020

- Page 4, 1st paragraph should read Chief Information Security Officer, not Chief Information System Officer.
- Page 5, 4th paragraph – Per NIST SP800-37 Revision 2, "Control assessments determine the extent to which the selected controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security and privacy requirements for the system and the organization."
- Page 5, B. CSCC ASSESSMENT DOCUMENT, the report states "In 2017, OPM included the CSCC controls testing as part of another system's independent assessment. Although the CSCC controls were independently assessed, we identified inconsistencies in the assessment results documentation." The OCIO would like to provide clarification on the content provided in the report. The draft report describes a list of deficient controls and conflicting information between two different reports. During the audit, the OCIO described the activities that occurred during the last assessment of controls that was conducted. The documents that were provided were not meant to be compared in the way portrayed in the report as there were multiple control assessments and risk evaluations which demonstrate an evolution of the risk assessment over time. The OCIO produced artifacts demonstrating the results of the original control evaluation and risk assessment as well as subsequent testing and risk assessment for the common controls. The overall result concluded that there were eight residual risks.
- Page 6, 2nd paragraph – Per NIST SP800-37 Revision 2, "The results of the security and privacy control assessments, including recommendations for correcting deficiencies in the implemented controls, are documented in the assessment reports."

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