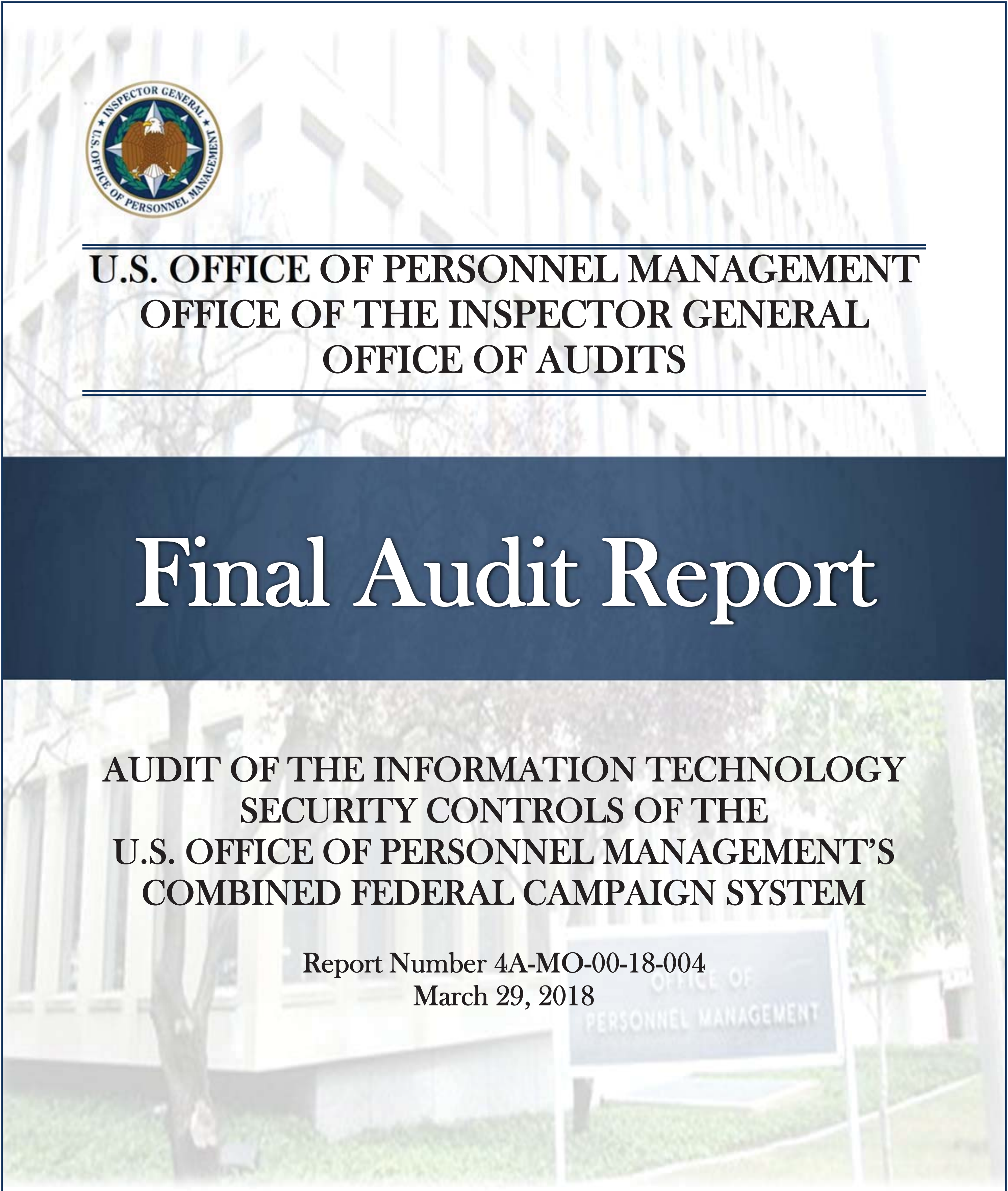

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S COMBINED FEDERAL CAMPAIGN SYSTEM

Report Number 4A-MO-00-18-004
March 29, 2018

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the
U.S. Office of Personnel Management's
Combined Federal Campaign System

Report No. 4A-MO-00-18-004 **March 29, 2018**

Why Did We Conduct the Audit?

The Combined Federal Campaign System (CFCS) is one of the U.S. Office of Personnel Management's (OPM) major Information Technology (IT) systems. The Federal Information Security Modernization Act (FISMA) requires 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 the CFCS 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 the CFCS determined that:

- A Security Assessment and Authorization of the CFCS was updated in December 2017. An Authorization to Operate was granted for up to two years.
- The security categorization of the CFCS 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 the CFCS.
- The CFCS System Security Plan generally follows the OCIO template, but there were instances where the documentation was inaccurate.
- An independent security controls assessment has been performed for the CFCS, but not all of the identified control weaknesses were included in the CFCS risk assessment.
- The CFCS has been subject to routine testing as part of OPM's continuous monitoring program.
- A contingency plan was developed and tested for the CFCS generally in compliance with NIST SP 800-34, Revision 1 and OCIO guidance.
- The CFCS Plan of Action and Milestones documentation did not identify weakness remediation deadlines.
- 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 two areas for improvement.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
CFCS	**Combined Federal Campaign System**
FedRAMP	**Federal Risk and Authorization Management Program**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
IG	**Inspector General**
IT	**Information Technology**
MSAC	**Merit System Accountability and Compliance**
NIST	**National Institute of Standards and Technology**
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**
SP	**Special Publication**
TASC	**Total Administrative Services Corporation**

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 U.S. Office of Personnel Management (OPM)'s FISMA compliance strategy and document the status of its compliance efforts.

The Combined Federal Campaign is a nation-wide donation program for Federal employees and retirees that is managed by OPM's Merit System Accountability and Compliance (MSAC) office. The Combined Federal Campaign System (CFCS) is used by charities to submit applications for inclusion in the Combined Federal Campaign, by donors to pledge charitable donations, and by MSAC for program administration including customer service and tracking receipts and disbursements.

OPM's Office of the Chief Information Officer (OCIO) and a contractor organization, Total Administrative Services Corporation (TASC), share responsibility for implementing and managing the information technology (IT) security controls of the CFCS. The CFCS resides in a Federal Risk and Authorization Management Program (FedRAMP) certified Cloud Service Provider. We discussed the results of our audit with OCIO and MSAC representatives at an exit conference. This was our first audit of the CFCS.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an evaluation of the security controls for the CFCS to ensure that the OCIO, MSAC, and TASC 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 have been implemented for the CFCS, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (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 Process (POA&M); 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 the CFCS, including the evaluation of IT security controls in place as of December 2017.

We considered the CFCS 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, MSAC, and TASC with security responsibilities related to the CFCS, 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 the CFCS 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 CFCS 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 I, Responsibilities for Protecting and Managing Federal 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, Revision 1, An Introduction to Information 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 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 that 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 (OIG), as established by the Inspector General Act of 1978, as amended. The audit was conducted from October through December 2017 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 CFCS 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

The CFCS has a current and valid 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 a current Authorization is required for every OPM system.

In November 2016 OPM granted an initial Authorization to Operate for the portion of the system that accepts and manages charity applications. This Authorization to Operate was good for up to three years and included requirements that the system owner monitor and remediate identified weaknesses on an ongoing basis. In October 2017 the system underwent a major change with the addition of the donor portal for submitting charitable pledges. In December 2017 the entire modified system received an Authorization to Operate for the remaining two years.

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

B. FIPS 199 ANALYSIS

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

NIST SP 800-60 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 CFCS security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The CFCS is assessed as having a “moderate” impact level for each area, resulting in an overall categorization of “moderate.”

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

C. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis of Federal information systems to determine if a Privacy Impact Assessment is required for that system. A Privacy Threshold Analysis was performed on the CFCS in September 2016, and it was determined that a Privacy Impact Assessment was required for this system.

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. The Privacy Impact Assessment was complete and was approved by the Chief Privacy Officer on October 13, 2017.

We did not detect any issues with the Privacy Impact Assessment performed for the CFCS.

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 for each system, and provides guidance for doing so.

The System Security Plan for the CFCS was developed using the OCIO’s System Security Plan template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires that the following elements be documented within the System Security Plan:

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

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

We reviewed the current System Security Plan for the CFCS and determined that it does not adequately address all of the requirements of NIST. Specifically, the system description does not properly identify the physical location of the CFCS.

With regards to a System Security Plan, 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 system documentation increases the risks that controls are not implemented and functioning as required. This increases the difficulty of assessing and addressing risks to the system and to OPM as a whole.

Recommendation 1

We recommend that OPM update the CFCS System Security Plan in accordance with the agency's policies and NIST standards.

OPM Response:

"We concur. According to the recommendation detail, this finding is centered on the fact that 'the system description does not properly identify the physical location of the CFCS.' The MSAC Program Office and OPM Cybersecurity will work with the contractor to have this updated prior to the January 28th response date that was requested by the OIG. The updated [System Security Plan] will be provided to the OIG once it is completed."

OIG Comment:

As a part of its response to the draft report, OPM provided an updated version of the System Security Plan that included the necessary corrections. No further action is required.

E. SECURITY ASSESSMENT PLAN AND REPORT

The CFCS Security Assessment Plan and Security Assessment Report were completed by an independent contractor in September and November of 2016, respectively, as a part of the system's Authorization process. We reviewed the related 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 assessment results table showed that 80 of the 256 controls tested were not fully satisfied. Of these 80 control deficiencies identified, 7 were not appropriately included in the risk assessment of the Security Assessment Report. The remaining 73 controls (those that were included in the risk assessment), were consolidated to 41 weaknesses and all appropriately added to the CFCS POA&Ms.

The CFCS risk assessment did not include seven known control weaknesses.

OPM's Authorization Guide requires that each weakness identified in the assessment be assessed for risk as a part of the Security Assessment Report.

Failure to assess the risk associated with all identified weaknesses increases the likelihood that weaknesses are not properly prioritized for remediation.

Recommendation 2

We recommend that OPM perform an analysis to assess the risk of the seven known control deficiencies that were omitted from the risk assessment. The CFCS risk assessment and POA&Ms should be updated to include all identified weaknesses and their risk levels.

OPM Response:

"We concur. According to the recommendation detail, seven controls were not appropriately included in the risk assessment of the [Security Assessment Report]. While we are not disputing this, MSAC [Program Management Office] and OPM Cybersecurity are requesting the OIG auditors provide the seven missing controls in order to complete a gap analysis prior to the [January] 28th response due date. If OPM cannot address the seven controls, we will ensure that a separate risk assessment is completed, if one has not already been done within the year that the system received an [Authorization to Operate]. These controls will also be added to our quarterly Continuous Monitoring."

OIG Comment:

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

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 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 did not detect any issues with the CFCS continuous monitoring submissions for fiscal year 2017.

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 CFCS contingency plan documents the functions, operations, and resources necessary to restore and resume the CFCS 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 CFCS 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 most recent contingency plan test for the CFCS was conducted in August 2017. The functional test was considered successful although the recovery took slightly longer than anticipated.

Nothing came to our attention to indicate that the CFCS 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.

1) Overdue POA&Ms

The CFCS has 41 security weaknesses identified on its POA&M, and 40 have scheduled completion dates that are over eight months overdue. While we understand that POA&Ms can be delayed due to resources constraints, it is imperative that POA&M documentation be updated so that the current risks to the system can be understood. The POA&M process is used to track the progress and the delays in the remediation of system weaknesses so that resources may be efficiently used when available.

All but one CFCS POA&M is over eight months past the scheduled remediation deadline.

OPM's POA&M Guide 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] 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] issued for the applicable system. Updated milestones and expected completion dates will be required for the following [Management Review Board] 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.

Recommendation 3

We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

OPM Response:

"We concur. MSAC [Program Management Office] and OPM Cybersecurity will work with the Contractor to develop an action plan to remediate all over[due] POA&M items."

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 the CFCS. 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;
- Configuration Management;
- Identity and Authentication;
- Risk Assessment;
- System and Communications Protection; and
- Audit and Accountability;
- Contingency Planning;
- Planning;
- Security Assessment and Authorization;
- System and Information Integrity.

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 tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements with the exceptions detailed below.

1) Control CM-6 – Configuration Settings

The CFCS security documentation states that the approved server configuration settings for the system follow the Defense Information Systems Agency's Security Technical Implementation Guide. Configuration settings are the system options that are adjusted to enforce or enhance protection of system components and data. We conducted configuration compliance scans on the servers supporting the CFCS to verify that the established settings had been properly applied. However, our scans found [redacted] configuration settings that were not in compliance with the Defense Information Systems Agency's Security Technical Implementation Guide.

NIST SP 800-53, Revision 4, states that "Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers . . . ." NIST requires that configuration settings be established and documented and any deviations be documented and approved.

Failure to apply established configuration settings increases the risk that hackers could exploit system weaknesses.

<u>Recommendation 4</u>

We recommend that OPM work with the FedRAMP Program Management Office to ensure that its Cloud Service Provider apply the approved security configuration settings for the CFCS.

<u>OPM Response:</u>

"We concur. MSAC [Program Management Office] and OPM Cybersecurity agree with the underlying issue of the recommendation. [The] CFCS utilizes a FedRAMP Certified Platform as a Service as its Cloud Service Provider. The [Cloud Service Provider] is [redacted] and they were granted their FedRAMP certification via the FedRAMP Joint Authorization Board. With this, the FedRAMP [Program Management Office] itself is responsible for monitoring the environment and ensuring that all security measures are implemented. With this oversight, the FedRAMP [Program Management Office] can review and approve exceptions to the [Defense Information System's Security Technical Implementation Guide] configurations and the Agency will have no say.

Our [Cloud Service Provider] is responsible for maintaining the entire infrastructure, to include Networking, Storage, Servers, Virtualization, O/S, Middleware and Runtime. The [redacted] server configuration settings that were identified are not items that OPM itself can remediate immediately via our tools or configuration updates.

Again, while we do feel it should be addressed, OPM has worked and will continue to work with the [Cloud Service Provider] to ensure that the secure configurations are implemented."

2) Control SI-2 – Flaw Remediation

We also conducted credentialed vulnerability scans on the servers supporting the CFCS looking for security weaknesses. The results of our scans indicate that several servers were missing critical patches that had been released more than 30 days before the scans took place. The specific weaknesses found by the scans were provided to OPM personnel, but will not be detailed in this report.

NIST SP 800-53, Revision 4, requires that, "The organization: . . . Identifies, reports, and corrects information systems flaws . . . [and] Installs security-relevant software and firmware updates . . . ."

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses.

<u>Recommendation 5</u>

We recommend that OPM work with the FedRAMP Program Management Office to ensure that its Cloud Service Provider applies system patches in a timely manner and in accordance with policy.

<u>OPM Response:</u>

"We concur. MSAC [Program Management Office] and OPM Cybersecurity do agree with the underlying issue of the recommendation. [The] CFCS utilizes a FedRAMP Certified Platform as a Service as its Cloud Service Provider. The [Cloud Service Provider] is [redacted] and they were granted their FedRAMP certification via the FedRAMP Joint Authorization Board. With this, the FedRAMP [Program Management Office] itself is responsible for monitoring the environment and ensuring that all security measures are implemented. With this oversight, the FedRAMP

[Program Management Office] can review and approve patch exceptions and the Agency will have no say.

Our [Cloud Service Provider] is responsible for maintaining all of the patching and infrastructure, to include Networking, Storage, Servers, Virtualization, O/S, Middleware and Runtime. OPM has worked and will continue to work with the [Cloud Service Provider] to ensure that the infrastructure is patched on a regular basis. If OIG can provide the name of the critical patches that were not implemented in a timely manner, OPM will notify the [Cloud Service Provider] and FedRAMP [Program Management Office] that timely patches are expected in the future."

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Merit System
Accountability and
Compliance

January 29, 2018

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: MARK W. LAMBERT
Associate Director, Merit System Accountability and Compliance

SUBJECT: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Combined Federal Campaign
(Report No. 4A-MO-00-18-004)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Combined Federal Campaign, 4A-MO-00-18-004.

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

Recommendation #1: We recommend that OPM updates the CFCS SSP in accordance with the agency's policies and NIST standards

We concur. According to the recommendation detail, this finding is centered on the fact that "the system description does not properly identify the physical location of the CFCS." The MSAC Program Office and OPM Cybersecurity will work with the contractor to have this updated prior to the January 28th response date that was requested by the OIG. The updated SSP will be provided to the OIG once it is completed.

Recommendation #2: We recommend that OPM perform an analysis to assess the risk of the seven known control deficiencies that were omitted from the risk assessment. The CFCS risk assessment and POA&Ms should be updated to include all identified weaknesses and their risk levels.

We concur. According to the recommendation detail, seven controls were not appropriately included in the risk assessment of the SAR. While we are not disputing this, MSAC PMO and OPM Cybersecurity are requesting the OIG auditors provide the seven missing controls in order to complete a gap analysis prior to the Jan 28th response due date. If OPM cannot address the seven controls, we will ensure that a separate risk assessment is completed, if one has not already been done within the year that the system received an ATO. These controls will also be added to our quarterly Continuous Monitoring.

Recommendation #3: We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

We concur. MSAC PMO and OPM Cybersecurity will work with the Contractor to develop an action plan to remediate all over POA&M items.

Recommendation #4:
We recommend that OPM apply the approved security configuration settings for the CFCS.

We concur. MSAC PMO and OPM Cybersecurity agree with the underlying issue of the recommendation. CFCS utilizes a FedRAMP Certified Platform as a Service as its Cloud Service Provider (CSP). The CSP is [redacted] and they were granted their FedRAMP certification via the FedRAMP Joint Authorization Board. With this, the FedRAMP PMO itself is responsible for monitoring the environment and ensuring that all security measures are implemented. With this oversight, the FedRAMP PMO can review and approve exceptions to the DISA STIG configurations and the Agency will have no say.

Our CSP is responsible for maintaining the entire infrastructure, to include Networking, Storage, Servers, Virtualization, O/S, Middleware and Runtime. The [redacted] server configuration settings that were identified are not items that OPM itself can remediate immediately via our tools or configuration updates.

Again, while we do feel it should be addressed, OPM has worked and will continue to work with the CSP to ensure that the secure configurations are implemented.

Recommendation #5: We recommend that OPM apply system patches in a timely manner and in accordance with policy.

We concur. MSAC PMO and OPM Cybersecurity do agree with the underlying issue of the recommendation. CFCS utilizes a FedRAMP Certified Platform as a Service as its Cloud Service Provider (CSP). The CSP is [redacted] and they were granted their FedRAMP certification via the FedRAMP Joint Authorization Board. With this, the FedRAMP PMO itself is responsible for monitoring the environment and ensuring that all security measures are implemented. With this oversight, the FedRAMP PMO can review and approve patch exceptions and the Agency will have no say.

Our CSP is responsible for maintaining all of the patching and infrastructure, to include Networking, Storage, Servers, Virtualization, O/S, Middleware and Runtime. OPM has worked and will continue to work with the CSP to ensure that the infrastructure is patched on a regular basis. If OIG can provide the name of the critical patches that were not implemented in a timely manner, OPM will notify the CSP and FedRAMP PMO that timely patches are expected in the future.

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

Report Fraud, Waste, and Mismanagement

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

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

By Phone:

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

By Mail:

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