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

Final Audit Report

Audit of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative

Report Number 4A-CI-00-19-008
October 23, 2019

EXECUTIVE SUMMARY

Audit of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative

Report No. 4A-CI-00-19-008 **October 23, 2019**

Why Did We Conduct The Audit?

Our primary objective was to evaluate the U.S. Office of Personnel Management's (OPM) compliance and reporting for the Federal Information Technology Reform Act's Data Center Optimization Initiative (DCOI) requirements. In conjunction with this audit, we also reviewed the information technology security controls and documentation for OPM's three general support systems. The Federal Information Security Modernization Act (FISMA) requires that the Office of the Inspector General (OIG) perform audits of IT security controls of agency systems.

What Did We Audit?

The OIG has completed a performance audit of OPM's DCOI compliance efforts to ensure that the Agency's efforts meet the requirements from the U.S. Office of Management and Budget, and that the security controls of selected systems meet the standards established by the FISMA, the National Institute of Standards and Technology, and OPM's Office of the Chief Information Officer.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit determined that:

<u>Data Center Optimization Initiative</u>
OPM has defined a DCOI Strategic Plan to consolidate its data center infrastructure, including closing data centers. However, this plan has not been updated since 2017 and does not address any of the other DCOI objectives or targets.

While OPM has closed several data centers according to its plan, the agency has not implemented the required tools to optimize its data centers. These include automated tools for monitoring, inventory, management, and power metering.

OPM has submitted the quarterly reports as required. However, some data elements from the reports are incorrect, including the number, closure status, and power utilization of the agency's data centers.

<u>General Support System (GSS) Security Controls</u>
Our review of the system security documentation for each of the GSSs identified numerous issues. OPM policy does not define what documents need to be updated and reviewed when an official in the assessment process leaves. Additionally, there are issues with the categorization, privacy assessments, risk assessments, weakness tracking, and security plans.

When reviewing the GSSs' security controls, we noted that all three GSSs data center spaces could not [redacted]. Additionally, the data center spaces at OPM's Washington, D.C. location do not have a control in place to detect and alert for the presence of water.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
DCOI	**Data Center Optimization Initiative**
ESI	**Enterprise Server Infrastructure**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
FITARA	**Federal Information Technology Acquisition Reform Act**
FY	**Fiscal Year**
GSS	**General Support System**
IG	**Inspector General**
IT	**Information Technology**
LAN/WAN	**Local Area Network/Wide Area Network**
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**
PIA	**Privacy Impact Assessment**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threat Analysis**
Q	**Quarter**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

In December of 2014, Congress passed the Federal Information Technology Acquisition Reform Act (FITARA) to give agency Chief Information Officers greater authority over information technology (IT) investments. This legislation established goals and responsibilities for improved IT risk management, transparency, and more effective IT investment oversight. FITARA updates the U.S. Office of Management and Budget's (OMB) Federal Data Center Consolidation Initiative. The new program is called the Federal Data Center Optimization Initiative (DCOI). Agencies are required to annually report and post online the following information:

- Comprehensive data center inventories;
- Strategy for achieving DCOI metrics;
- Performance metrics;
- Timelines for agency activities; and
- Cost calculation, including investments and cost savings.

The OMB issued Memorandum M-16-19 as guidance for agencies to use when working to comply with the DCOI. It identifies agencies' goals, requirements, and criteria for this effort. The memorandum states that "rooms with at least one server, providing services (whether in a production, test, staging, development, or any other environment) are considered data centers." Furthermore, M-16-19 defines tiered data centers as those that utilize: "1) a separate physical space for IT infrastructure; 2) an uninterruptible power supply; 3) a dedicated cooling system or zone; and 4) a backup power generator for prolonged power outages."

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

As part of this evaluation, we reviewed the U. S. Office of Personnel Management's (OPM) FISMA compliance strategy and documented the status of its compliance efforts. In conjunction with the data center review above, we reviewed system documentation and security controls for OPM's three General Support Systems (GSS).

OPM's Local Area Network / Wide Area Network (LAN/WAN) GSS provides both local and wide area connections for OPM employees and contractors. Some of the sub-systems in the LAN/WAN GSS include OPM's Development and Test Environment, OPM's Voice over Internet Protocol, and OPM's Web Platform. This system has components located in Washington, D.C.; Macon, Georgia; and Boyers, Pennsylvania.

The Enterprise Server Infrastructure (ESI) GSS is OPM's mainframe environment. This environment supports various IT systems used by OPM's program offices: OPM's National Background Investigations Bureau, the Office of the Chief Financial Officer, and Retirement Services. This system is located in Washington, D.C.

The Macon GSS is the infrastructure environment that supports OPM's Human Resources Solutions collection of systems including USAJobs, USAStaffing, and a data warehouse. This system is located in Macon, Georgia.

The LAN/WAN GSS, ESI GSS, and Macon GSS support all of OPM's internally hosted major information systems. While OPM does have some cloud systems, the majority of OPM's systems are internal, and these GSSs provide key security controls for the confidentiality, integrity, and availability of the supported agency systems.

While we have audited the agency for FITARA compliance, this is our first audit evaluating the DCOI requirements. We have audited the security controls and documentation of the GSSs in prior audits. Our prior audit reports titled *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's CTS General Support System*, Report 4A-CI-00-11-043, and *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Server Infrastructure General Support System*, Report 4A-CI-00-11-016, assessed the controls for the Macon GSS and ESI GSS, respectively. These prior reports and all of the associated recommendations were closed. In addition, our prior reports titled *Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Local Area Network / Wide Area Network General Support System*, Report 4A-CI-00-12-014, and *Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology,* Report 4A-CI-00-17-014, assessed the controls in place for the LAN/WAN GSS. Some of the recommendations from the latter report are still open. We have incorporated the previous recommendations into section III of this report.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objectives were to: 1) perform an evaluation of OPM's IT programs and procedures for compliance with FITARA's DCOI requirements and OMB guidance, and 2) to evaluate the security controls for OPM's three general support systems in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and OPM's Office of the Chief Information Officer (OCIO).

The audit objectives were accomplished by reviewing the degree to which OPM has implemented and reported on FITARA requirements for the DCOI. In combination, we also reviewed the security program elements implemented for the support systems, including the:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards Publication (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 Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related agency policies and procedures, compliance testing, and other audit procedures that we considered necessary. The audit scope covered OPM's FITARA DCOI compliance efforts and OPM's FISMA compliance for its three GSSs. This audit is a continuation of our review of OPM's compliance with FITARA that began with the *Audit of the U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act*, Report 4A-CI-00-18-037. The combined DCOI and FISMA compliance scope evolved from a natural overlap in subject areas, with an objective to achieve resource efficiencies, and address an area of high risk identified through prior FISMA audits.

We considered OPM's 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 objectives, we reviewed relevant OPM IT policies and procedures, Federal laws, and OMB policies and guidance. We interviewed representatives of OPM's OCIO. We also reviewed documentation including historical reports, system security documentation, and tested system controls.

The findings, recommendations, and conclusions outlined in this report are based on the current status of OPM's compliance with FITARA as of March 2019, and are located in the "Audit Findings and Recommendations" section of this report. Since our audit would not necessarily disclose all significant matters in relation to FITARA or FISMA compliance, we do not express an opinion on OPM's compliance as a whole, only the sections of FITARA determined to be in scope for this audit, as detailed above.

Various laws, regulations, and industry standards were used as a guide for evaluating audit documentation and interviews. These criteria include, but are not limited to, the following publications:

- Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015 (P. L. 113-291), Title VIII, Subtitle D, Federal Information Technology Acquisition Reform;

- OMB Memorandum M-16-19, Data Center Consolidation Initiative;

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

- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-37, Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems and Organizations;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

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

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

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

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. The audit was conducted in accordance with Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The audit was performed by the OPM OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from October 2018 through March 2019 in OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's compliance with FITARA and FISMA is consistent with applicable standards. OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. DATA CENTER OPTIMIZATION INITIATIVE COMPLIANCE

1. DCOI Strategic Plan

OMB M-16-19 requires agencies to annually create and post online their strategic plans to meet the requirements of the DCOI. This plan is to include “at a minimum, the following:

1. Planned and achieved performance levels for each optimization metric, by year;

2. Planned and achieved closures, by year;

3. An explanation for any optimization metrics and closures for which the agency did not meet the planned level in a previous Strategic Plan;

4. Year-by-year calculations of target and actual agency-wide spending and cost savings on data centers from fiscal years (FY) 2016 through 2018, including:

    a. A description of any initial costs for data center consolidation and optimization; and

    b. Life cycle cost savings and other improvements (including those beyond FY 2018, if applicable);

5. Historical costs, cost savings, and cost avoidances due to data center consolidation and optimization through FY 2015; and

6. A statement from the agency [Chief Information Officer] stating whether the agency has complied with all reporting requirements in this memorandum and the data center requirements of FITARA. If the agency has not complied with all reporting requirements, the agency must provide a statement describing the reasons for not complying.”

In addition, the OMB guidance states that agencies were to target closing 25 percent of tiered data centers and 60 percent of non-tiered data centers by the end of FY 2018, and in the long term to close all non-tiered data centers.

OPM’s DCOI plan was last updated in 2017.

OPM’s DCOI plan has two components and was last updated on its website in 2017. The written component outlines the consolidation from nine data centers spread out across multiple locations to two in Macon, Georgia and Boyers, Pennsylvania; and the numerical component provides reporting of planned and achieved goals by year. OPM projected the consolidation efforts to be completed by the end of FY 2018. While OPM's written plan focuses on outlining the consolidation efforts for major data centers, it does not detail plans for accomplishing the optimization goals of the DCOI (facility utilization rates, energy metering, virtualization rates, and automated monitoring), and does not identify tiered versus non-tiered data centers for closure. The numerical component of the plan does identify some of the required goals; however, without the support of a complete and well-documented plan, these goals are not likely to be realized.

Failure to meet the planning requirements of DCOI increases the risk that agency resources will be used inefficiently and that agency goals will not be in line with Federal requirements.

Recommendation 1

We recommend that OPM update its DCOI plan to include all aspects required by DCOI and OMB guidance.

Management Response:

"We concur with your recommendation. OPM will review and assess the current DCOI plan and update as needed per DCOI and OMB guidance."

OIG Comments:

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.

2. Data Center Closures

As mentioned above, the stated target for each agency is to reduce the number of tiered data centers by 25 percent. Tiered data centers, as defined by OMB, "utilize each of the following: 1) a separate physical space for IT infrastructure; 2) an uninterruptable power supply; 3) a dedicated cooling system or zone; and 4) a backup power generator for prolonged power outages." Per OMB, agencies are to self-classify data centers and any "Data centers previously classified as tiered in past inventories will automatically be classified as tiered under the DCOI."

OPM's Strategic Plan outlines the consolidation of OPM's infrastructure starting from nine data centers (defined in the inventory as seven agency data centers and two non-agency operated facilities), down to two agency data centers by the end of FY 2018.

During our audit, we toured multiple OPM facilities and identified that OPM has consolidated equipment from four of the seven data centers identified for closure in the strategic plan. This represents a greater than 40 percent reduction in the number of data centers from OPM's position at the start of the DCOI.

3. Data Center Optimization

Automated Monitoring

OMB M-16-19 states, "Agencies shall replace manual collections and reporting of systems, software, and hardware inventory housed within data centers with automated monitoring, inventory, and management tools (e.g., data center infrastructure management) by the end of [FY] 2018."

Our FY 2018 FISMA Report included a series of recommendations (Recommendations 5, 8, 9, and 10) to improve OPM's management of its systems, hardware, and software inventories. These recommendations remain open, and it is likely that the agency will have to address these FISMA recommendations before it can implement automated tools for infrastructure management.

Failure to have automated monitoring, inventory, and management tools increases the risk that agency resources are not efficiently used and increases the likelihood a system is not appropriately accounted for in the environment. Understanding the environment and associated systems is necessary for implementing security and privacy controls to reduce the risk of unauthorized data exposure and data loss, and to maintain availability.

Recommendation 2

We recommend that OPM perform a gap analysis to identify the monitoring, inventory, and management tools that it needs to implement automated infrastructure management as required by the DCOI and OMB.

Management Response:

"We concur with your recommendation. OPM will perform a gap analysis to assist in evaluating automated infrastructure tools for possible implementation."

Power Metering

OMB M-16-19 mandates that, "Agencies shall install automated energy metering tools and shall use these to collect and report energy usage data in their data centers to OMB." The March 19, 2015, Executive Order 13693, "Planning Federal Sustainability in the Next Decade," requires agencies to install and monitor advanced energy meters in data centers by September 30, 2018.

OPM does not have energy metering installed in all of its data centers. The process for collecting power usage data for OPM's data centers is not well defined, involves manual collection of data, and some estimating. Advanced power metering tools are necessary to enable the active tracking of power usage effectiveness for the data centers.

Failure to maintain automated power metering at data centers and the corresponding lack of data increases the risk of inefficiently using agency resources and impairs the ability of agency officials to plan effectively.

Recommendation 3

We recommend that OPM install automated power metering in all of its data centers in accordance with the requirements in the DCOI.

Management Response:

"We concur with your recommendation. OPM will implement power metering in the OPM Macon Data Center. OPM will be migrating equipment from the Washington D.C. Distributed Data Center and Boyers Data Center into the new OPM space at the Iron Mountain Data Center. The Iron Mountain Data Center employs automated power metering."

4. Reporting

OMB requires quarterly submissions to measure the agency’s progress towards the optimization, power usage, and closure metrics. Reporting on these metrics is required for all agency data centers.

OPM has complied with OMB’s request, providing quarterly submissions. However, the submissions from Quarter (Q)1 FY 2017 through Q4 FY 2018 do not provide an accurate representation of OPM’s data center inventory or DCOI compliance. Examples of the inaccuracies are detailed below.

Despite OPM’s DCOI submissions only listing one data center in Macon, our tour of the Macon facility identified four distinct spaces that meet the DCOI reporting requirements for data centers. As such, OPM DCOI submissions should report that the Macon facility encompasses three tiered and one non-tiered data centers.

Additionally, OPM has inaccurately reported data centers as closed that are currently in use. During our tour of OPM’s data center space in Washington, D.C., we observed that one of the spaces that was reported as closed had active IT assets. We confirmed that OPM has production systems running in that data center. The other data center incorrectly reported as closed was the ESI GSS backup facility. The contingency plan for the ESI GSS identifies that data center as active and lists the installed OPM equipment. We confirmed the active status of this data center in the contract with the 3rd party data center provider.

OPM is not currently reporting the correct number of open data centers in its quarterly submissions.

Lastly, the power utilization and effectiveness metrics that OPM has been reporting are inaccurate. We compared the reported usage across the submissions and noted that the reported usage does not change from quarter to quarter for many of the data centers despite the fact that the number of servers in each changed drastically as the data centers were consolidated. In one data center, the electrical usage was almost unchanged from the initial report even though the server count had dropped to zero in the latest report. In another data center, the usage had remained exactly the same even when the server count had more than doubled. We confirmed with agency personnel that there was not a defined process for collecting the information nor was there documentation about how the information had been determined historically.

Failure to accurately report DCOI metrics increases the risk that agency resources will be used inefficiently, and that agency goals and resources will not align with Federal requirements.

Recommendation 4

We recommend that OPM assess the current state of its infrastructure to accurately report data center metrics, including the correct number of data centers (including non-tiered spaces), the correct operational status of data centers, and accurate energy usage.

Management Response:

"We concur with your recommendation. OPM will review and assess current state and report accurate data center metrics in the next quarterly DCOI report."

B. GENERAL SUPPORT SYSTEMS

NIST defines a general support system as "an interconnected set of information resources under the same direct management control that shares common functionality." As noted above, OPM's system inventory identifies three GSSs: the Local Area Network / Wide Area Network GSS (LAN/WAN), the Enterprise Server Infrastructure (ESI) GSS, and the Macon GSS. Our evaluation of the GSSs' security controls for compliance with established IT security policies and procedures is discussed below:

1. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) includes 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I mandates that all Federal information systems have a valid Authorization. OPM Policy requires an Authorization for all OPM systems at least once every three years. The findings and recommendations from our review of the OPM GSSs' Authorizations are discussed below.

Macon General Support System

The Macon GSS was granted an Authorization in October 2016. This Authorization is valid for up to three years, included requirements that the system owner monitor and remediate identified weaknesses on an ongoing basis, and expires in October 2019.

ESI General Support System

The ESI GSS was granted an Authorization in October 2017. This Authorization is valid for up to two years, included requirements that the system owner monitor and remediate identified weaknesses on an ongoing basis, and expires in October 2019.

LAN/WAN General Support System

The LAN/WAN GSS was granted an Authorization in October 2017. This Authorization is valid for up to two years, included requirements that the system owner monitor and remediate identified weaknesses on an ongoing basis, and expires in October 2019.

However, for each of the GSSs, there is a new authorizing official since the most recent Authorization was signed. When a system is inherited by a new authorizing official, the system must be reauthorized.

NIST SP 800-37, Revision 1, requires that "In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decisions document, authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision . . . formally [accepting] responsibility and accountability . . . and explicitly accepting the risk . . . ."

OPM's current Authorization policies and procedures do not define requirements for addressing a change in authorizing official. Specifically, OPM's documentation does not require a new authorizing official to review system documentation and sign a new Authorization decision as required by NIST SP 800-37, Revision 1.

OPM's current policies do not address when there is a change in authorizing official.

Failure to update a system's documentation and Authorization when an official in the Authorization process leaves increases the risk that the system will operate without proper risk management oversight and accountability.

Recommendation 5

We recommend that OPM update its Authorization policies and procedures to include requirements for reauthorizing systems in the event of a change in authorizing official. This guidance at a minimum should include parameters for the time period for re-authorization and requirements to evidence the system documentation reviews required by NIST.

Management Response:

"We concur with your recommendation. OPM will update its policies to allow for new Authorizing Officials to review the authorization package in the event of a change to the Authorizing Official for information systems. The corresponding authorization package review would determine if a new [Authority to Operate] is required."

Recommendation 6

We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization decision for the Macon GSS.

Management Response:

"We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation [5]. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation [5]."

Recommendation 7

We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization decision for the ESI GSS.

Management Response:

"We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation [5]. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation [5]."

Recommendation 8

We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization decision for the LAN/WAN GSS.

Management Response:

"We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation [5]. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation [5]."

2. FIPS 199 Categorization

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. The Federal Information Processing Standards (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 the FIPS 199 Publication. The GSSs' security categorization documentation analyzes information processed by the systems and the corresponding potential impact on confidentiality, integrity, and availability. The findings and recommendations from our review of the OPM GSSs' security categorizations are discussed below.

Macon General Support System

The Macon GSS is assessed as having a "moderate" impact level for each area, resulting in an overall categorization of "moderate." Our review of the system categorization from the prior Authorization noted that the document was not properly signed. Additionally, since the drafting of the Authorization, the Macon GSS now supports a major information system with a "high" categorization.

NIST SP 800-18, Revision 1, describes the concept of high water mark for security categorization, and specifies that a GSS should be marked at the highest categorization level for the major systems that it supports.

Failure to categorize a GSS according to the high water mark standard increases the risk that proper controls will not be identified and implemented for the protection of sensitive and private information.

Recommendation 9

We recommend that OPM categorize the Macon GSS as a high system and conduct a gap analysis to verify that the additional controls required for a high system are in place.

Management Response:

"We do not concur with your recommendation. In accordance with the [FISMA], [OMB] Circular A-130, Appendix I-4, states that for security categorization, agencies shall:

1) ***Identify authorization boundaries for information systems in accordance with NIST SPs 800-18 and 800-37; and***

2) ***Categorize information and information systems, in accordance with FIPS Publication 199 and NIST SP 800-60, considering potential adverse security and privacy impacts to organizational operations and assets, individuals, other organizations, and the Nation.***

Consequently, OPM follows SP 800-18 and 800-37 to identify the authorization boundaries, but then uses [FIPS] 199 and guidance in [SP] 800-60 Revision 1 to

categorize the security level of its systems. Using the standards articulated in FIPS 199 and SP 800-60, OPM has categorized the Macon GSS as a moderate system. OPM will continue to follow NIST standards and guidelines and its policies and procedures for determining the appropriate security categorization for its systems."

<u>OIG Comments:</u>

We agree that OPM should follow NIST SP 800-18 and SP 800-60 guidance for categorizing its major information systems. It is important to note that the guidance provides additional language specific to evaluating a GSS. NIST SP 800-18 states, "A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting." NIST SP 800-60 Volume 1 further explains the necessity to use the high water mark to determine a GSS's categorization, stating "Since networks, as well as other general support systems, do not inherently 'own' mission-based or management and support information types, the infrastructure's categorization is based on the aggregation of the information systems' security categorizations. In other words, the infrastructure's security categorization is the high water mark of the supported information systems and is based on the information types processed, flowed, or stored on the network or general support system." We continue to recommend that OPM categorize the Macon GSS as a high system and to conduct a gap analysis to verify that the additional controls required for a high system are in place.

ESI & LAN/WAN General Support Systems

The ESI GSS is assessed as having a "moderate" to "high" impact level for each area, resulting in an overall categorization of "high." The LAN/WAN GSS is assessed as having a "high" impact level for each area, resulting in an overall categorization of "high."

For both GSSs, the categorization documents were signed by the authorizing officials in 2015, but were not signed by the CISO until 2018. Since the original signature in 2015, the systems underwent new Authorizations by different authorizing officials. The security categorizations should have been updated, reviewed, and approved by the current authorizing officials at the time of the Authorization.

The most recent security categorization for both the ESI and LAN/WAN GSSs were not approved by the current authorizing official.

As noted above, NIST SP 800-37, Revision 1, requires that "In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the ongoing monitoring activities."

Failure to update and approve the FIPS 199 increases the risk that system changes and their affects are not appropriately documented, and this increases the risk that sufficient controls are not in place to protect the system and data.

Since the entire authorization packages must be reviewed and approved by the current authorizing officials as discussed above in Recommendations 7 & 8, no additional recommendations are needed to address these identified weaknesses.

3. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis (PTA) of Federal information systems to determine if a Privacy Impact Assessment (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. The findings and recommendations from our review of the OPM GSSs' PIAs are discussed below.

Macon General Support System

A PTA was performed on the Macon GSS in September 2016 and it was determined that a PIA was required for this system. However, the Macon GSS received an authorization without having a completed PIA.

OPM policy requires all systems to receive a PTA to assess the need for a PIA. Failure to identify systems with sensitive data increases the risk that proper controls will not be implemented to protect the data from accidental disclosure.

OPM identified this issue and created a POA&M during FY 2018; no further recommendations will be made.

ESI & LAN/WAN General Support Systems

In the most recent Authorizations, the ESI GSS's PTA was not complete (i.e., it did not indicate whether a PIA is required) or approved and the LAN/WAN GSS package did not include a PTA. PIAs for both GSSs were not provided during the course of the audit.

The E-Government Act of 2002 states that an agency must "conduct a privacy impact assessment," and the agency must also "ensure the review of the privacy impact assessment [is completed] by the Chief Information Officer, or equivalent . . . ."

Failure to complete the privacy impact assessment process increases the risk that sensitive information will not be identified and documented. Without this documentation there is an increased risk that the proper controls will not be selected to protect that information from unauthorized disclosure or use.

Recommendation 10

We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the ESI GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.

Management Response:

"We concur with your recommendation. OCIO will work with the Office of Privacy and Information Management to complete required privacy documentation."

Recommendation 11

We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the LAN/WAN GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.

Management Response:

"We concur with your recommendation. OCIO will work with the Office of Privacy and Information Management to complete required privacy documentation."

4. System Security Plan

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

OPM developed an SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires SSPs to contain the following elements:

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

The findings and recommendations from our review of the OPM GSSs' SSPs are discussed below.

Macon General Support System

We reviewed the current Macon GSS SSP, signed on November 5, 2018, and determined that it does utilize the OPM template; however, the SSP does not adequately address all of the requirements of NIST. Specifically, the hardware and software inventory is not defined in the appendices.

NIST SP 800-18, Revision 1, states that "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."

Failure to maintain an accurate hardware and software inventory in the SSP increases the difficulty of assessing and addressing risks to the system and to OPM as a whole. This also increases the likelihood that all risks were not considered while reviewing the Authorization.

Recommendation 12

We recommend that OPM update the Macon GSS SSP to reflect the current state of the system and ensure it meets NIST guidelines.

Management Response:

"We concur with your recommendation. The system security plan was updated to remove the reference to an electronic system. The inventories now reside as separate documents, attached to the system security plan. The inventories are provided with this response."

OIG Comments:

OPM provided an updated SSP and inventories in its draft report response that addresses the recommendation. No further action is required.

ESI General Support System

We reviewed the current ESI GSS SSP dated September 22, 2016, and determined that it does utilize the OPM template; however, the Chief Information Officer and Authorizing Official at the time of the Authorization in 2016 did not sign and approve the SSP.

Additionally, we determined the SSP is incomplete. Specifically, there is a connection to the Sterling Forest backup site that is not sufficiently documented in the SSP. The SSP does note that the Sterling Forest facility acts as a data backup site, but it does not document any of the security and privacy controls in place. Nor does it fully identify how the backup site is part of the authorization boundary for ESI GSS.

The ESI GSS SSP does not sufficiently document the alternate storage and processing site in Sterling Forest.

NIST SP 800-18, Revision 1, states that the authorizing official must "review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system."

Failure to maintain current and complete system documentation increases the risk that controls are not implemented and functioning as required. Without reviewing and approving the security plan the authorizing official may not have a complete understanding of the system's risk before acceptance.

Recommendation 13

We recommend that OPM update and approve the ESI SSP to include all of the necessary information to fully document the Sterling Forest site.

Management Response:

"We concur with your recommendation. OPM will update and approve the ESI SSP to include all of the necessary information to fully document the Sterling Forest site."

LAN/WAN General Support System

In the *Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology*, Report 4A-CI-00-17-014, we identified several critical issues with the LAN/WAN GSS SSP. We identified that the security controls selection was not accurate, that the SSP did not adequately define the system environment, and that the inherited controls were not properly documented.

The SSP was updated in 2017 after the draft reporting process of the prior audit. From our review, we noted that there had been some improvement in the controls documentation and the control selection no longer appears to be an issue. However, the other issues identified in the prior report continue to exist. In addition to the missing inventories identified in the prior report, the LAN/WAN GSS SSP still does not show the current system environment. Critical elements such as the physical locations of data centers and descriptions of the security tools in place are missing. The third issue noted in the prior audit report continues to be an issue as controls are listed as inherited without evidence to support the control inheritance. This is verified by our NIST SP 800-53, Revision 4, control testing discussed in section 9 below; we identified two control weaknesses for the LAN/WAN GSS which are both documented in the SSP as "inherited."

NIST, OMB, and OPM policies all require that systems have documented security plans. Failure to keep the SSP information current increases the likelihood that security and privacy controls are not properly implemented across a system's entire boundary.

Our prior recommendation for addressing the issues in the LAN/WAN SSP is still open, so no additional recommendations are necessary.

5. Security Assessment Plan and Report

One of the key components to the risk management and Authorization processes is an assessment of risk. At the system level this is done by assessing the controls in place and their effectiveness. OPM's process requires the development of a Security Assessment Plan (SAP) to identify systems components, the controls assessment methodology, and the individuals performing the assessment. The SAP is then used to conduct independent control testing. The results identify weaknesses which are then documented in a Security Assessment Report (SAR), assessed for risk, and documented in the system's POA&Ms. The findings and recommendations from our review of the OPM GSSs' SAPs and SARs are discussed below.

Macon General Support System

The Macon GSS SAP and SAR were completed in September 2016 as 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 verified that appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization.

We identified one weakness in the control testing that was not subsequently included in the risk assessment and did not have a documented risk acceptance. There were 10 weaknesses evaluated in the risk assessment, 8 of which were mitigated, leaving only 2 open weaknesses. The two open weaknesses were appropriately added to the Macon GSS POA&Ms, however the weakness missing from the control assessment was not added.

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

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

Recommendation 14

We recommend that OPM perform a gap analysis for the Macon GSS to assess the risk of the omitted control deficiency and update the POA&Ms to include all identified weaknesses.

Management Response:

"We concur with your recommendation. The control in question is being evaluated as a part of a new security assessment. Any risks associated with the implementation of the control will be documented and tracked within a corresponding POA&M."

ESI General Support System

The ESI GSS SAP and SAR were completed in July and August 2016, respectively, as 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 "High" security categorization.

The assessment results table showed that there were 21 controls that were not fully satisfied. Additionally, there were eight controls that did not have a documented control assessment, and subsequently were not assessed for risk. Also, there were two weaknesses assessed for risk that were not appropriately included in the POA&Ms.

OPM's Authorization Guide requires that each applicable control must be tested and each identified weakness must be assessed for risk as part of the SAR. Failure to assess the risk associated with all identified weaknesses increases the likelihood that weaknesses are not properly prioritized for remediation.

Recommendation 15

We recommend that OPM perform a gap analysis for the ESI GSS to assess the risk of the omitted control deficiencies and update the POA&Ms to include all identified weaknesses.

Management Response:

"We concur with your recommendation. A gap analysis will be performed on the omitted ESI GSS controls and risk assessed. Any identified deficiencies or weaknesses will be documented and tracked within a corresponding POA&M."

LAN/WAN General Support System

In the *Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology*, Report 4A-CI-00-17-014, we identified several critical issues with the LAN/WAN GSS SAP and SAR. These issues included the testing scope, the system documentation provided to the assessors, and constraints on the assessment. The identified issues limit the effectiveness of the LAN/WAN GSS risk assessment. Failure to identify and assess system risk increases the likelihood that limited resources are not utilized in an efficient manner to address the risks to the system.

Our recommendation to re-perform the assessment is still open, so no additional recommendations are necessary.

6. Continuous Monitoring

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template identifying the security controls that must be tested for each information system based on its security categorization. The test results must be provided to the OCIO on a routine basis for centralized tracking. The findings and recommendations from our review of the OPM GSSs' continuous monitoring processes are discussed below.

Macon & ESI General Support Systems

We received quarterly continuous monitoring submissions for both the Macon and ESI GSSs. A review of the submissions revealed that for each of the GSSs over 100 distinct controls were tested in accordance with the documented schedule.

For both GSSs, while the test work was generally well documented, in some cases the resulting decision on the efficacy of the controls was missing or deviated from the template.

Despite this documentation issue, nothing came to our attention to indicate that the Macon GSS or ESI GSS continuous monitoring process was inadequate.

LAN/WAN General Support System

OPM's LAN/WAN GSS has not been subject to continuous monitoring since 2017.

OPM's LAN/WAN GSS has not been subjected to continuous monitoring since 2017. In response to further inquiry the OCIO acknowledged that this was a resource constraint issue. The FY 2018 FISMA report includes Recommendation 46 for identifying resources gaps in the continuous monitoring program. This recommendation has not been closed.

7. 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.

i. Contingency Plan

NIST SP 800-34, Revision 1, states that a system contingency plan "provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system." The findings and recommendations from our review of the OPM GSSs' contingency plans are discussed below.

Macon General Support System

The Macon GSS contingency plan was updated in June 2018 and it documents the functions, operations, and resources necessary to restore and resume the Macon GSS 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 Macon GSS contingency plan.

ESI General Support System

The ESI GSS contingency documentation was most recently updated in April 2018 and signed in August 2018. While the document does not follow the OPM template, it documents the functions, operations, and resources necessary to restore and resume the ESI GSS.

We did not detect any issues with the ESI GSS contingency plan.

LAN/WAN General Support System

The current LAN/WAN GSS Contingency Plan is dated June 2014, and has not been updated on an annual basis as required. The contingency plan does not accurately reflect the current environment since the system infrastructure has undergone significant changes in the last five years (e.g., adding and removing data centers and systems).

The LAN/WAN GSS contingency plan has not been updated since 2014.

NIST SP 800-34, Revision 1, states "As a general rule, the [Information System Contingency Plan] should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the [Information System Contingency Plan], system, mission/business processes supported by the system, or resources used for recovery procedures." Documenting plan approvals by the system owner is another critical step.

Failure to have an updated contingency plan increases the risk that OPM will not have proper resources and procedures to address incidents and minimize the impact of adverse events.

Recommendation 16

We recommend that OPM update and approve the contingency plan for the LAN/WAN GSS.

Management Response:

"We concur with your recommendation. The LAN/WAN Contingency Plan will be reviewed and updated."

ii. 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 organizations readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results. The findings and recommendations from our review of the OPM GSSs' contingency plan tests are discussed below.

Macon & ESI General Support Systems

The most recent contingency plan tests for Macon GSS and ESI GSS were conducted in June and May of 2018, respectively.

The intent of the Macon GSS test was to simulate a re-deployment of the system's major and minor applications. The Macon GSS functional test was considered successful and had documented lessons learned to limit downtime of the system. The ESI GSS test included the major systems that are hosted on the mainframe platform, and was also considered successful and had documented lessons learned.

We did not identify any issues with either the Macon GSS or ESI GSS contingency plan testing.

LAN/WAN General Support System

As discussed above, OPM's LAN/WAN GSS contingency plan has not been updated in approximately five years and the LAN/WAN GSS environment has changed significantly in that time. Contingency plan testing is not effective when plans do not represent the current environment, system, and facilities.

Failure to test a contingency plan increases the risk that identified procedures or resources are not sufficient to mitigate likely risks in disaster incidents.

Recommendation 17

We recommend that OPM test the updated LAN/WAN contingency plan.

This recommendation cannot be completed until Recommendation 16 has been implemented.

Management Response:

"We concur with your recommendation. Once the LAN/WAN Contingency Plan is reviewed and updated a Contingency Plan Test will be conducted."

8. 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. The findings and recommendations from our review of the OPM GSSs' POA&M processes are discussed below.

Macon, ESI, & LAN/WAN General Support Systems

The Macon GSS, ESI GSS, and LAN/WAN GSS POA&Ms are generally documented according to OPM policy. However, OPM failed to adhere to remediation dates for its POA&M weaknesses.

At the time of this audit, the Macon GSS did not have overdue POA&Ms. However, for the ESI GSS 65 of the 104 POA&Ms were overdue by more than six months. For the LAN/WAN GSS, there were 57 open weaknesses dating back to FY 2012. All 57 weakness remediation plans are past their estimated completion dates.

In the *Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology*, Report 4A-CI-00-17-14, we identified that the LAN/WAN GSS POA&M documentation had not been appropriately included when the system was authorized. Our recommendation from that report is still open.

OPM's guidance states "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 update the 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.

During the *Federal Information Security Modernization Act Audit Fiscal Year 2018*, Report 4A-CI-00-18-038, we identified POA&M closure deadlines as a weakness and rolled forward the recommendation from 2016. This recommendation is still open.

Recommendation 18

We recommend that OPM identify the necessary resources or process changes to ensure that POA&Ms are updated according to policy.

Management Response:

"We partially concur with your recommendation as OPM has already internally conducted the recommended analysis and continue to work on other corrective actions communicated during OIG fieldwork for the [FY] 2019 Federal Information Security Modernization Act. In June 2019, we completed a five day [POA&M] Sprint to evaluate the current state and outstanding requirements of the open POA&Ms and to reduce the agency's inventory of open POA&Ms. The sprint was structured to provide for planning, requirement dissemination, and program specific closure sessions. A memorandum outlining additional information regarding this effort is provided with this response."

OIG Comments:

In the FY 2018 FISMA report, we reported that a significant number of OPM's POA&Ms had not been updated with current information. As a part of its response to the draft audit report, OPM provided evidence of its POA&M sprint in June and demonstrated continued improvement to its POA&Ms. However, the need to perform sprints to catch up on outdated POA&Ms can be indicative of systemic resource and management issues. We continue to recommend that OPM identify the necessary resources or process changes to ensure that POA&Ms are updated according to policy.

9. NIST SP 800-53 Evaluation

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the Federal government. As part of this audit, we evaluated whether OPM has implemented a subset of these controls. For each of the GSSs, we tested approximately 30 controls as outlined in NIST SP 800-53, Revision 4, including controls from the following control families:

- Access Control;
- Configuration Management;
- Audit and Accountability;
- Contingency Planning;

- Identity and Authentication;
- Incident Response;
- Maintenance;
- Media Protection;
- Physical and Environmental Protection;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection; and
- 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 majority of the tested security controls appear to be in compliance with the requirements of NIST SP 800-53, Revision 4, with the exceptions discussed below.

i. Control PE-3(1) – Physical Access Control | Information System Access

Macon, ESI, & LAN/WAN General Support Systems

During our tours of the three data centers that support the Macon, ESI, and LAN/WAN GSSs we noted that OPM had not implemented [redacted].

None of OPM's data center locations have [redacted].

The data centers in Macon, Georgia have an [redacted], but it is not in use by OPM.

The data centers in Washington, D.C. and Boyers, Pennsylvania have not implemented any [redacted].

NIST SP 800-53, Revision 4, provides guidance for [redacted]

[redacted]

Failure to implement [redacted] The agency's overall risk profile is adversely compounded because not only does the control weakness put the data from these systems at risk, but also all of the systems they support. As this weakness was identified for all three OPM GSSs, every system technically supported by the agency is subject to this weakness.

Recommendation 19

We recommend that OPM implement [redacted] at the data centers located in Macon, Georgia.

Management Response:

"We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover."

OIG Comments:

As stated above, NIST requires that organizations enforce security controls to authorize each individual accessing both the facility and sensitive areas such as data centers. OPM's own control policy requires both facility level and sensitive area level access controls. The policy states that the agency is to "Enforce physical access authorizations to the information system in addition to the physical access controls for the facility at [data centers]." Enforcing [redacted] to data centers reduces the risk of insider threats and unauthorized access to sensitive information. As mentioned above, Macon now supports a major information system with a high categorization due to the information it contains. In addition, the Macon facility has [redacted] that is in place but not operational. We continue to recommend that OPM implement [redacted] at the data centers located in Macon, Georgia.

Recommendation 20

We recommend that OPM implement [redacted] at the data centers located in Washington, D.C.

Management Response:

"We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover."

OIG Comments:

In addition to our comments after the response to Recommendation 19 above, we would also point out that the Washington, D.C. data centers house multiple systems with a high categorization. As such, we continue to recommend that OPM implement [redacted] at the data centers located in Washington, D.C.

Recommendation 21

We recommend that OPM implement [redacted] at the data centers located in Boyers, Pennsylvania.

Management Response:

"We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover."

OIG Comments:

In addition to our comments after the response to Recommendation 19 above, we would also point out that the Iron Mountain data center space is not operated by OPM, [redacted]. We continue to recommend that OPM implement [redacted] at the data centers located in Boyers, Pennsylvania.

ii. Control PE-13(3) – Fire Protection | Automatic Fire Suppression

Macon & LAN/WAN General Support Systems

Our evaluation of the Macon GSS's risk assessment identified that control enhancement PE-13(3) had been omitted. We confirmed that the data center space in the Macon facility does not have a functional automatic fire suppression system. There is a fire detection system and some of the components for an automatic suppression system have been installed, but at the time of this report the system is not in operation. Although OPM stated that it has accepted this risk, the requested risk acceptance documentation was not provided. This weakness affects both the Macon GSS and the LAN/WAN GSS housed in the Macon facility.

NIST SP 800-53, Revision 4, requires that "The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis." Failure to employ adequate fire suppression capabilities increases the risk of loss of life and data if an incident occurred.

Recommendation 22

We recommend that OPM implement an automatic fire suppression system at the data centers located in Macon, Georgia.

Management Response:

"We concur with your recommendation. The automatic fire suppression system has been installed in the Macon data center and fully tested as of June 7, 2019. A record of the installation of the system is provided with this response."

OIG Comments:

OPM provided evidence of the installed suppression system. No further action is required.

iii. Control PE-15 (1) – Water Damage Protection | Automation Support

ESI & LAN/WAN General Support Systems

During our tour of OPM's Washington, D.C. data centers, we did not identify water detection devices. Despite system documentation for both the ESI and LAN/WAN GSSs indicating the control was inherited from OPM's facilities office, OPM later confirmed that the control is not in place.

NIST SP 800-53, Revision 4, states that "The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts . . . [organization personnel] . . . ." Failure to implement automated water detection increases the risk of system damage if a water source leaks into the data center space.

Recommendation 23

We recommend that OPM implement automated water detection controls in the Washington, D.C. data centers.

Management Response:

"We concur with your recommendation. OPM will evaluate automated water detection capabilities for the Washington, D.C. data center with consideration for planned transition efforts."

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

July 30, 2019

MEMORANDUM FOR [redacted]
Chief, Information System Audits Group
Office of Personnel Management
Office of the Inspector General

FROM: CLARE A. MARTORANA
Chief Information Officer
Office of Personnel Management

SUBJECT: Audit of the U.S. Office of Personnel Management's
Compliance with the Data Center Optimization Initiative
(Report No. 4A-CI-00-19-008)

Thank you for providing the Office of Personnel Management (OPM) the opportunity to respond to the Office of the Inspector General (OIG) draft report, Compliance with the Data Center Optimization Initiative (Report No. 4A-CI-00-19-008)

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

Recommendation #1: We recommend that OPM update its DCOI plan to include all aspects required by DCOI and OMB guidance.

Management Response: We concur with your recommendation. OPM will review and assess the current DCOI plan and update as needed per DCOI and OMB guidance.

Recommendation #2: We recommend that OPM perform a gap analysis to identify the monitoring, inventory, and management tools that it needs to implement automated infrastructure management as required by the DCOI and OMB.

Management Response: We concur with your recommendation. OPM will perform a gap analysis to assist in evaluating automated infrastructure tools for possible implementation.

Recommendation #3: We recommend that OPM install automated power metering in all of its data centers in accordance with the requirements in the DCOI.

Management Response: We concur with your recommendation. OPM will implement power metering in the OPM Macon Data Center. OPM will be migrating equipment from the Washington D.C. Distributed Data Center and Boyers Data Center into the new OPM space at the Iron Mountain Data Center. The Iron Mountain Data Center employs automated power metering.

Recommendation #4: We recommend that OPM assess the current state of its infrastructure to accurately report data center metrics including the correct number of data centers (including non-tiered spaces), correcting closing status of data centers, and energy usage.

Management Response: We concur with your recommendation. OPM will review and assess current state and report accurate data center metrics in the next quarterly DCOI report.

Recommendation #5: We recommend that OPM update its Authorization policies and procedures to include requirements for reauthorizing systems in the event of a change in authorizing official. This guidance at a minimum should include parameters for the time period for re-authorization and requirements to evidence the system documentation reviews required by NIST.

Management Response: We concur with your recommendation. OPM will update its policies to allow for new Authorizing Officials to review the authorization package in the event of a change to the Authorizing Official for information systems. The corresponding authorization package review would determine if a new ATO is required.

Recommendation #6: We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization to Operate for the Macon GSS.

Management Response: We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation 4. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation 4.

Recommendation #7: We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization to Operate for the ESI GSS

Management Response: We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation 4. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation 4.

Recommendation #8: We recommend that the current authorizing official review the prior Authorization package and any updated system documentation and issue a current Authorization to Operate for the LAN/WAN GSS.

Management Response: We partially concur with your recommendation. OPM understands and agrees with the need to have a new Authorizing Official re-evaluate authorizations, per our concurrence with Recommendation 4. The current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document (as OIG recommends), reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with its updated policies described in Recommendation 4.

Recommendation #9: We recommend that OPM categorize the Macon GSS as a high system and conduct a gap analysis to verify that the additional controls required for a high system are in place.

Management Response: We do not concur with your recommendation. In accordance with the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) Circular A-130, Appendix I-4, states that for security categorization, agencies shall:

1) Identify authorization boundaries for information systems in accordance with NIST SPs 800-18 and 800-37; and
2) Categorize information and information systems, in accordance with FIPS Publication 199 and NIST SP 800-60, considering potential adverse security and privacy impacts to organizational operations and assets, individuals, other organizations, and the Nation.

Consequently, OPM follows SP 800-18 and 800-37 to identify the authorization boundaries, but then uses Federal Information Processing Standard (FIPS) 199 and guidance in Special Publication (SP) 800-60 Revision 1 to categorize the security level of its systems. Using the standards articulated in FIPS 199 and SP 800-60, OPM has categorized the Macon GSS as a moderate system. OPM will continue to follow NIST standards and guidelines and its policies and procedures for determining the appropriate security categorization for its systems.

Recommendation #10: We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the ESI GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.

Management Response: We concur with your recommendation. OCIO will work with the Office of Privacy and Information Management to complete required privacy documentation.

Recommendation #11: We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the LAN/WAN GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.

Management Response: We concur with your recommendation. OCIO will work with the Office of Privacy and Information Management to complete required privacy documentation.

Recommendation #12: We recommend that OPM update the Macon GSS SSP to reflect the current state of the system and ensure it meets NIST guidelines.

Management Response: We concur with your recommendation. The system security plan was updated to remove the reference to an electronic system. The inventories now reside as separate documents, attached to the system security plan. The inventories are provided with this response.

Recommendation #13: We recommend that OPM update and approve the ESI SSP to include all of the necessary information to fully document the Sterling Forest site.

Management Response: We concur with your recommendation. OPM will update and approve the ESI SSP to include all of the necessary information to fully document the Sterling Forest site.

Recommendation #14: We recommend that OPM perform a gap analysis for the Macon GSS to assess the risk of the omitted control deficiency and update the POA&Ms to include all identified weaknesses.

Management Response: We concur with your recommendation. The control in question is being evaluated as a part of a new security assessment. Any risks associated with the implementation of the control will be documented and tracked within a corresponding POA&M.

Recommendation #15: We recommend that OPM perform a gap analysis for the ESI GSS to assess the risk of the omitted control deficiencies and update the POA&Ms to include all identified weaknesses.

Management Response: We concur with your recommendation. A gap analysis will be performed on the omitted ESI GSS controls and risk assessed. Any identified deficiencies or weaknesses will be documented and tracked within a corresponding POA&M.

Recommendation #16: We recommend that OPM update and approve the contingency plan for the LAN/WAN GSS.

Management Response: We concur with your recommendation. The LAN/WAN Contingency Plan will be reviewed and updated.

Recommendation #17: We recommend that OPM test the updated LAN/WAN contingency plan. This recommendation cannot be completed until Recommendation 16 has been implemented.

Management Response: We concur with your recommendation. Once the LAN/WAN Contingency Plan is reviewed and updated a Contingency Plan Test will be conducted.

Recommendation #18: We recommend that OPM identify the necessary resources or process changes to ensure that POA&Ms are updated according to policy.

Management Response: We partially concur with your recommendation as OPM has already internally conducted the recommended analysis and continue to work on other corrective actions communicated during OIG fieldwork for the fiscal year 2019 Federal Information Security Modernization Act. In June 2019, we completed a five day Plan of Action and Milestones (POA&M) Sprint to evaluate the current state and outstanding requirements of the open POA&Ms and to reduce the agency's inventory of open POA&Ms. The sprint was structured to provide for planning, requirement dissemination, and program specific closure sessions. A memorandum outlining additional information regarding this effort is provided with this response.

Recommendation #19: We recommend that OPM implement [redacted] at the data centers located in Macon, Georgia.

Management Response: We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover.

Recommendation #20: We recommend that OPM implement [redacted] at the data centers located in Washington, D.C.

Management Response: We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover.

Recommendation #21: We recommend that OPM implement [redacted] at the data centers located in Boyers, Pennsylvania.

Management Response: We do not concur with your recommendation. OPM requires from its security policy numerous controls to prevent unauthorized access, which are implemented and periodically tested. OPM considers its controls sufficient to provide adequate limitation of physical access to information systems, equipment, and the respective operating environments to authorized individuals. Due to the sensitive nature of these controls, we are not outlining such controls in this response. However, we can provide more information to OIG about such controls under separate cover.

Recommendation #22: We recommend that OPM implement an automatic fire suppression system at the data centers located in Macon, Georgia.

Management Response: We concur with your recommendation. The automatic fire suppression system has been installed in the Macon data center and fully tested as of June 7, 2019. A record of the installation of the system is provided with this response.

Recommendation #23: We recommend that OPM implement automated water detection controls in the Washington, D.C. data centers.

Management Response: We concur with your recommendation. OPM will evaluate automated water detection capabilities for the Washington, D.C. data center with consideration for planned transition efforts.

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