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 SECURITY ASSESSMENT AND AUTHORIZATION METHODOLOGY

Report Number 4A-CI-00-20-009
September 18, 2020

EXECUTIVE SUMMARY

Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology

Report No. 4A-CI-00-20-009 **September 18, 2020**

Why Did We Conduct The Audit?

In fiscal year (FY) 2018, the Office of the Inspector General reported a significant deficiency in the Office of Personnel Management's (OPM) security assessment and authorization process. While there was a valid Security Assessment and Authorization (Authorization) in place for almost every major information technology (IT) system in the agency's system inventory, the quality of the work and supporting documentation was questionable. We performed this audit to evaluate the effectiveness of OPM's Authorization program.

What Did We Audit?

Our objectives were to review OPM's current Authorization methodology and to evaluate a judgmental sample of Authorization packages.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

OPM has made improvements in the authorization process for systems since the FY 2016 Authorization sprint. We believe OPM has addressed the significant deficiency in its Authorization process as it has documentation for each system we observed. While OPM has made positive efforts in improving its Authorization process as systems are reauthorized, OPM has not shown the ability to consistently perform routine continuous monitoring activities. Our audit found:

- OPM has adequate policies, procedures, and templates for the Information System Security Officers and the System Owners to follow.
- Authorization memoranda were approved and signed prior to expiration for all but Serena Business Manager, which has not been updated within the agency defined periods.
- OPM's guidance for categorizing high value assets is unclear. Furthermore, seven system categorizations failed to receive the appropriate approvals and reviews based on OPM policy.
- Privacy Threshold Analyses and Privacy Impact Assessments are not consistently completed prior to a system's Authorization.
- System Security Plans are not consistently reviewed annually, and the master control sets are missing Plan of Action and Milestones (POA M) data.
- OPM's security control assessments contained multiple issues.
- Quarterly continuous monitoring submissions are consistent with our findings in our Federal Information Security Modernization Act audits as multiple systems did not perform valid testing in the fourth quarter of FY 2019.
- Contingency Planning activities are performed in an ad-hoc manner. Annual testing is not regularly performed, recovery metrics are inconsistent, and plans aren't updated annually.
- POA&Ms are defined but many are in initial or draft status for over six months and do not have milestones or estimated completion dates assigned.
- All prior audit recommendations remain open.

ABBREVIATIONS

AO	**Authorizing Official**
ATO	**Authorization to Operate**
Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Assessment**
CISO	**Chief Information Security Officer**
CP	**Contingency Planning**
Cyber GSS	**Cyber General Support System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
HVA	**High Value Asset**
I&N Tools	**Infrastructure and Networking Tools**
ISCM	**Information System Continuous Monitoring**
ISSO	**Information System Security Officer**
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**
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 Threshold Analysis**
SBM	**Serena Business Manager**
SO	**System Owner**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

APPENDIX: OPM's August 4, 2020, response to the draft audit report, issued July 6, 2020.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

The 2002 Federal Information Security Management Act requires: (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of Inspector General 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.

An information system Security Assessment and Authorization (Authorization) is a comprehensive assessment that evaluates whether a system's security controls are meeting the security requirements of that system. The purpose of this assessment is to document the system's controls, risks, and remediation plans. If the security risks associated with the system are deemed to be acceptable, then the system is formally authorized to operate in the agency's production information technology (IT) environment.

From fiscal years (FY) 2014 – 2016, our FISMA audits identified a material weakness in the U.S. Office of Personnel Management's (OPM's) Authorization process due to incomplete and inconsistent Authorization packages. In FY 2016 the Agency executed an Authorization Sprint designed to bring all of the agency's systems into compliance with Authorization requirements. This effort led to the majority of information systems receiving an authorization to operate (ATO). We subsequently conducted an audit of OPM's Authorization methodology and evaluated OPM's progress in addressing the material weakness. Due to various findings in that audit, we continued to believe that OPM's management of system Authorizations represented a material weakness in the internal control structure of the agency's IT security program. In the FY 2017 FISMA report, we upgraded the material weakness to a significant deficiency due to the agency's continued efforts to maintain Authorizations for all information systems. The significant deficiency was again reported in the FY 2018 FISMA report and we chose not to report on it in the FY 2019 FISMA audit report. This audit will assess the current status of OPM's Authorization methodology.

This was our second audit of the OPM Authorization Methodology. The previous audit resulted in four findings and recommendations documented in Report No. 4A-CI-00-17-014, dated June 20, 2017. All of the recommendations from the previous audit remain open.

OPM's Office of the Chief Information Officer (OCIO), Office of Privacy and Information Management, and each program office share responsibility for implementing and managing the IT security controls of all OPM systems. We discussed the results of our audit with the OCIO and the Office of Privacy and Information Management representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objectives were to review OPM's Authorization methodology and to evaluate the effectiveness of OPM's Authorization program. We achieved our objectives by evaluating the components of a judgmental sample of Authorization packages to determine if they were completed in accordance with applicable standards. We also assessed OPM's progress towards implementing the recommendations from the FY 2017 audit of OPM's Authorization methodology.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary.

The scope of this audit included a review of a judgmental sample of 15 Authorization packages. To select our sample, we established a goal to select a cross-section of the 47 systems in OPM's FISMA system inventory to identify trends in documentation and processes. We selected at least one system managed by each program office, Information System Security Officer (ISSO), and Authorizing official. Our selection included internal and contractor systems as well as low, moderate, and high systems. With our scope defined, we selected a total of 13 information systems. However, during fieldwork, we were informed one of the systems selected, the Local Area Network/Wide Area Network (LAN/WAN), was to be decommissioned and replaced with five component systems. We selected three of the five component systems to oversee the Authorization process as the systems were to be granted an ATO. The results of our audit do not project to the rest of the FISMA major system inventory. To accomplish our objective, we reviewed federal laws, OMB policies and guidance, National Institute of Standards and Technology (NIST) guidance, OPM IT policies and procedures, and relevant Authorization documentation. This audit covered the continuous monitoring and FISMA compliance efforts of OPM officials responsible for the Authorization process in place as of April 2020.

The findings, recommendations, and conclusions are located in the "Audit Findings and Recommendations" section of this report. Various laws, regulations, and industry standards were used as a guide for evaluating OPM's control structure. The criteria used in conducting this audit include:

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;

- Federal Information System Controls Audit Manual;
- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems;
- NIST Special Publication (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 800-39, Managing Information Security Risk: Organization, Mission, and Information System View;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 1, Volume II, 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;
- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002;
- OPM Contingency Planning Policy;
- OPM Continuous Monitoring Policy;
- OPM Plan of Action and Milestone Guide;

- OPM Privacy Impact Assessment Guide;
- OPM Security Authorization Guide;
- OPM Security Authorization Policy;
- OPM Security Planning Policy; and
- P.L. 113-283, Federal Information Security Modernization Act of 2014.

In conducting the audit, we relied, to varying degrees, on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, we conducted the audit in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The OPM Office of the Inspector General performed the audit, as established by the Inspector General Act of 1978, as amended. We conducted the audit from November 2019 through April 2020 at OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's management of the Authorization process 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. AUTHORIZATION PROGRAM STATUS

An Authorization includes 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. However, OPM does not yet have a mature program in place to continuously monitor system security controls, therefore an Authorization is required for all OPM systems at least once every three years as required by OPM policy.

We do not believe that the Authorization process represents a significant deficiency in OPM's information security program

As part of the prior Security Assessment and Authorization methodology audit, we determined that OPM's management of system Authorizations represented a material weakness in the internal control structure of the agency's IT security program. OPM has subsequently made improvements to its Authorization program by defining roles and responsibilities for personnel involved in the Authorization process. We determined that while OPM has adequate policies, procedures, and templates to assist personnel in updating and maintaining required Authorization documentation, there were multiple instances where the policies and procedures were not consistently applied across every system Authorization. However, we do not believe that the Authorization process currently represents a significant deficiency in OPM's information security program.

B. POLICIES AND PROCEDURES

OPM has developed policies that define the roles and responsibilities of all employees that assist in the Authorization process. The policies were created using guidance from FISMA, FIPS, OMB, and NIST. OPM's Security Authorization Policy describes the responsibilities for the ISSO, System Owner (SO), Authorizing Official (AO), and Chief Information Security Officer (CISO). The policy defines the elements of the Authorization package and which Official is responsible for each task. The policy assigns responsibilities for the security authorization, security categorization, privacy impact, and security assessments.

OPM has also created policies for each major component of an Authorization package. These policies include a Security Planning policy which describes the roles and responsibilities for creating and maintaining a System Security Plan (SSP). The ISSO is responsible for developing

the SSP while the SO must support in the development and maintenance of the SSP. The Contingency Planning policy provides the frequency and responsibilities of the SO to perform contingency planning activities. The Continuous Monitoring Policy defines the responsibilities of the ISSO to conduct ongoing security status monitoring of the system inventory and plan of action and milestones (POA&Ms) metrics for each system.

OPM developed guides to further assist ISSOs in the Authorization process. OPM had developed a Security Authorization and Assessment Guide that describes the roles and authorities in the Authorization process. The guide also provides a checklist of deliverables. Each Authorization package is required to have every element on the checklist to be eligible to receive a three year ATO. OPM also has a Privacy Impact Analysis (PIA) Guide for evaluating privacy risks and a POA&M Guide that details the lifecycle of a POA&M from the risk assessment to closure.

We have reviewed OPM's policies and procedures and believe that they provide a solid foundation for OPM's Authorization process. While some of the policies and guides have not been reviewed and updated within the agency-defined timeframe, we believe that the Authorization process should be effective if the guidance provided by OPM is appropriately and consistently applied.

C. AUTHORIZATION MEMORANDUM

The Authorization memorandum is the document that formally establishes a system's authority to operate in OPM's production IT environment. It is signed by the AO after they assess all of the risks to the systems that are documented in the Risk Assessment Report and the POA Ms. We reviewed the Authorization memoranda for the 15 systems in the scope of the audit to determine if they were valid and signed by the AO. All of the systems we reviewed have a valid Authorization memorandum except for the Serena Business Manager (SBM).

The SBM was granted a 120 day ATO on October 30, 2019. The ATO expired on February 27, 2020. The shortened ATO was granted because SBM is considered a mission critical application despite the fact that the independent assessor did not perform a thorough risk assessment. Within the 120-day period, OPM was supposed to perform the security control assessment and update all required documentation. OPM did not reassess and authorize SBM prior to the most recent ATO expiration. The necessary resources were not appropriated to review and assess all required controls, and documentation was not updated in a timely manner. We have not received evidence to support that this assessment was performed. The most recently approved assessment was performed in FY 2016.

The SBM Authorization package also has documentation that was either incomplete or not updated in a timely manner. The Privacy Threshold Analysis (PTA) and PIA have expired, the contingency plan failed to identify the proper recovery time objective, and the last contingency plan test was performed well outside of the required annual timeframe.

NIST SP 800-30, Revision 1, states, "Organizations use the results from risk assessments to help determine the severity of such vulnerabilities which in turn, can guide and inform organizational risk responses (e.g., prioritizing risk response activities, establishing milestones for corrective actions)." NIST SP 800-53, Revision 4, states that the organization should update the security authorization at an organization-defined frequency.

Without a complete risk assessment, the AO could accept unknown exploitable risks that could result in data loss or breach. This would also hinder the AO's ability to properly prioritize risk response activities.

Recommendation 1

We recommend that OPM perform a full assessment for SBM and update all Authorization documentation in accordance with NIST guidance.

OPM Response:

"We concur that a full assessment must be conducted. The OCIO will coordinate with supported business offices to obtain the resources needed to conduct the assessment and update appropriate documentation."

OIG Comment:

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

D. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. FIPS 199 provides guidance on how to assign appropriate categorization levels for information security according to a range of risk levels. NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to

Security Categories, provides an overview of the security objectives and impact levels identified in FIPS 199.

OPM maintains a FIPS 199 template which provides ISSOs with a specific format for documenting the types of information stored, processed, or transmitted by the system, the potential impact of the loss of confidentiality, integrity, and availability of those information types, and the overall system categorization. The template also contains signature lines for the CISO, AO, and SO. OPM also has a worksheet template which the ISSOs complete to evaluate whether a system is a High Value Asset (HVA).

Although we received a system categorization for each system, we believe that OPM can improve its system categorization process. The following sections detail our review of the FIPS 199 security categorization documentation:

We believe that OPM can improve its system categorization process.

1. Incorrect System Categorization

Of the 15 FIPS 199 security categorization documents reviewed, two systems which were categorized as moderate-impact systems were identified as HVAs. The HVA worksheet identified a rating of high in either confidentiality or integrity for both systems. FIPS 199 states, "For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system." OPM contests that the HVA designation does not affect the system categorization. However, OPM's HVA template suggests otherwise.

OPM's HVA template provides instruction on how to update the security categorization template based on a systems HVA status. The template states that the ISSO must "Adjust the System Categorization with the new HVA Information Type." FIPS 200 states, "The selected set of security controls must include one of three, appropriately tailored security control baselines from NIST Special Publication 800-53, Revision 4, that are associated with the designated impact levels of the organizational information systems as determined by the security categorization process."

Failure to properly categorize the systems could increase the risk that adequate security controls are not selected and tested, leaving sensitive assets vulnerable.

Recommendation 2

We recommend that OPM update its policies and procedures to include guidance on categorizing HVA systems.

OPM Response:

"We do not concur. OPM implemented its current security categorization process and template based on the Office of Management and Budget (OMB) memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. The first objective in this memorandum includes the identification of High Value Assets (HVAs). Although the Federal Information Processing Standard (FIPS) 199 is referenced in the memorandum, the process for identification of HVAs and the security categorization process are distinct. Each process has its own set of requirements and it is known by the Federal cybersecurity community that having a system go through the HVA identification process and come out as an HVA does not mean that the system will be identified as a High impact system using the FIPS 199 process. When OPM built its template, it was at the forefront of blending the two. The intent was to have the information in one location; however, at no point are processes for identifying HVA and High impact systems conjoined. The HVA worksheet template, as designed by the OPM OCIO, has not been used incorrectly from the intended purpose and has not led to the incorrect categorization of an OPM system."

OIG Comment:

We acknowledge that OPM has implemented its security categorization process based on OMB and CSIP guidance and agree that the HVA identification and FIPS 199 security categorization processes can be distinct. However, OPM's current guidance is confusing due to the language in the HVA template and the fact that the HVA identification and FIPS 199 categorization processes are combined into one template. We therefore made the recommendation to update/clarify policies and procedures instead of reclassifying the two systems referenced above. OPM's current guidance in the HVA template states that the ISSO must "Adjust the System Categorization with the new HVA Information Type." FIPS 199 guidance states that system criticality should match the highest watermark given the in the analysis of the system categorization. When the current HVA template language is combined with the FIPS security categorization document, the high watermark of the system is unclear.

We therefore continue to recommend that OPM update its policies and procedures to include guidance on categorizing HVA systems.

2. Missing Approvals

We observed seven security categorization documents that were not signed by all necessary personnel. The ISSO is responsible for documenting the security categorization using the prescribed templates and ensuring that the document is reviewed and approved. In failing to acquire the proper signatures, the ISSOs for these seven systems did not comply with OPM's Security Authorization Guide.

We observed seven security categorization documents that were not signed by all necessary personnel.

OPM's Security Authorization Policy states that the ISSO must "Ensure that the security categorization is reviewed and approved by the authorizing official or authorizing official designated representative[.]" OPM's Security Authorization Guide specifies that the SO, the CISO, and the AO approve the security categorization of the system.

Failure to properly approve categorization of the systems could increase the risk that adequate security controls are not selected and tested, leaving sensitive assets vulnerable.

Recommendation 3

We recommend that OPM have the SO, the CISO, the AO, and (where appropriate) the Chief Privacy Officer review and approve the categorization of the systems in its inventory, in accordance with agency policy.

OPM Response:

"We concur. The work conducted in this area has led to security categorizations signed in accordance with OPM policies and procedures for the vast majority of the major systems within its inventory. The OCIO will coordinate with OPM offices to collect the signatures necessary in accordance with its policies and procedures."

E. PRIVACY IMPACT ASSESSMENT

The E-Government Act of 2002 requires agencies to perform a 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.

OPM maintains a PIA template that was created using the components referenced in OMB Memorandum M-03-22. The template specifically identifies what information is to be collected, why the information is being collected, the intended use of the information, and how the information will be secured.

We believe that OPM has an opportunity to improve its process for reviewing and approving PTAs and PIAs. We observed that 5 of the 15 systems did not have a valid PTA and 3 systems that house personal data did not have a valid PIA. Furthermore, the ISSO and Chief Privacy Officer did not complete and approve the PTA and/or PIA within the defined timeframes within OPM's policy.

OPM's Security Authorization Guide states that "Federal agencies must conduct a [PTA] and possibly a [PIA] before developing or procuring an IT system or project that collects, maintains, or disseminates information in identifiable form from or about members of the public." In addition, the OPM PIA Guide states, "All OPM IT systems must have a PTA."

The OPM PIA Guide says, "Federal Information Security Management Act (FISMA) reporting requires [SOs] to review their PIAs every year and document whether there are any changes to the system." Further, the guide says that a PIA must be conducted "Every 3 years for existing systems without changes."

Failure to properly identify privacy information within a system increases the risk that Personally Identifiable Information will not be sufficiently protected.

This finding is consistent with the open recommendation in the FY 2019 FISMA audit report (Report No. 4A-CI-00-19-029, Recommendation 34) that recommends that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of personal data.

F. 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 maintains an SSP template that uses NIST SP 800-18, Revision 1, as guidance.

We observed that ISSOs are not effectively updating SSPs according to OPM policy. The following represents our assessment of OPM's SSPs:

We observed that ISSOs are not effectively updating SSPs according to OPM policy.

1. System Security Plan

We reviewed the SSP and master control set of the 15 systems in scope. Of the SSPs reviewed, we found issues with nine systems. We identified the following:

- Seven instances where the documents did not have the current AO and/or SO signature on the respective SSP;
- Two instances where the documents were last signed in 2018; and
- Three instances where the documents had missing/inaccurate information.

Our fieldwork indicates that the SSPs are not being reviewed and updated timely because OPM does not have an SSP review process in place for the ISSOs.

NIST SP 800-18, Revision 1, states, "All plans should be reviewed and updated, if appropriate, at least annually." NIST SP 800-18, Revision 1, also states that changes in AO and SO should trigger an update to the SSP. The OPM Security Authorization Guide states that "The ISSO is responsible for preparing the SSP for approval by the AO."

Without an annual review of the SSP, there is a risk that the AO and SO will be unaware of system changes that may be significant.

Recommendation 4

We recommend that OPM develop and implement a process to perform annual quality reviews for SSPs. The process should include the elements defined in NIST SP 800-18, Revision 1.

OPM Response:

"We concur. We will finalize documentation in the form of a Standard Operating Procedure (SOP) to ensure the annual review occurs consistently. Please refer to the provided technical comments."

2. Master Control Set

OPM has a template for evaluating SSP master control sets. The ISSO uses this document to define how controls are implemented for the system and scope the testing for the independent security controls assessment. Of the 15 systems reviewed, 7 systems had master control set fields that were incomplete or missing and contained planned controls that did not have corresponding POA&M references. The ISSOs are not updating all fields of the master control set appropriately with all defined controls.

OPM's Security Authorization guide states, "The ISSO is responsible for updating the SSP with the functional details of the security controls." OPM's Security Planning Policy states that the ISSO must "Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments."

If planned controls are not properly identified by the ISSO, an incomplete master control set can lead to the AO accepting unidentified risks and leave OPM vulnerable to potential exploits.

Recommendation 5

We recommend that OPM routinely ensure that all SSP master control sets are updated with POA&M references.

OPM Response:

"We do not concur. The OIG states, 'If planned controls are not properly identified by the ISSO, an incomplete master control set can lead to the AO accepting unidentified risks and leave OPM vulnerable to potential exploits.'

However, the System Security Plan (SSP) is not used as a document to communicate risk to the Authorizing Official. OPM uses other materials, including the Risk Assessment Table (RAT), Risk Assessment Report (RAR), Plan of Action and Milestones (POA&M), and a recommendation letter to provide applicable risk information to the Authorizing Official in order for the official to make an authorization decision. When an Authorizing Official review and makes a risk determination and authorization, the SSP and a POA&M line item would not lead to '... the AO accepting unidentified risks and leave OPM vulnerable to potential exploits." The Authorizing Official is provided a complete set of materials before making such decisions.'

OIG Comment:

During fieldwork, OPM expressed that the SSP Master Control Set is used to scope the testing of controls when performing the independent assessment. The assessor and ISSO would look to this document to make decisions on what controls need to be tested and which controls can be scoped out due to inheritance or if a control is an agency common control. If this document is not updated annually to accurately depict the state of the system, there is a chance that a control that should be tested is missed during the independent assessment, which would affect the results of the RAT and RAR. As mentioned above, the AO reviews this documentation before accepting the overall risk to the system.

We continue to recommend that OPM routinely ensure that all SSP master control sets are updated with POA&M references.

G. SECURITY ASSESSMENT PLAN AND REPORT

We identified at least one issue with each system's security assessment plan and report.

A security assessment plan describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls. The results of the security control assessment are captured within the Assessment Results Table. A risk assessment is performed for each weakness following NIST SP 800-30, Revision 1, guidance using the Risk Assessment Table. The results of the risk assessment are compiled into the Risk Assessment Report. We do not believe that OPM is accurately or effectively scoping and testing all required controls for a system.

OPM policy requires routine risk assessments for each system as part of the Authorization process. OPM has defined the policies and procedures for testing controls and the associated risk assessment for individual systems. We reviewed assessment documentation for 15 of OPM's major systems. We identified at least one issue with each system. We observed incomplete security control assessments where multiple controls were not assessed. Additionally, there were instances where the security assessment plan failed to document controls that were out of scope. We observed inconsistencies between the control testing weaknesses and risks identified. There were also instances where the AO's review and approval was not documented.

The ISSO is responsible for the completeness and accuracy of the security assessment plan, execution of the assessment results table, and is accountable for the risk assessment table and risk assessment report. OPM's ISSOs appear unable to provide consistent oversight of the security control assessment to ensure that all required controls are assessed for risk and

weaknesses are identified. This issue is compounded by the inaccuracies in the system security categorization and SSP.

During the FY 2019 FISMA Audit, OPM cited that they have performed an ISSO service requirement gap analysis and have identified that they require more ISSOs. OPM has added a few more ISSOs to help manage their information systems. The hiring of new ISSOs should be accompanied with adequate training on the Authorization process for new and current ISSOs.

OPM's Security Authorization Guide says that the risk assessment "will determine the residual risk remaining in the system that the Authorizing Official will need to accept to authorize the system to operate."

NIST SP 800-39 states, "Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations."

Failure to adequately assess all system controls and system risks increases the possibility that weaknesses will not be identified in the system controls or that the information will not be incorporated when determining whether a system should be authorized to operate.

Recommendation 6

We recommend that OPM improve the training program for new and current ISSOs on OPM's Authorization process. Training should include guidance on how to provide proper oversight related to security control scoping and risk identification and documentation.

OPM Response:

"We concur. OPM agrees with the OIG position on this recommendation and we have identified strategic hiring needs within the ISSO role and other positions that contribute to these functions. OPM will update the guidance provided in its training for ISSOs upon obtaining the necessary resources."

H. CONTINUOUS MONITORING

OPM's Continuous Monitoring Policy, created using guidance from NIST SP 800-53, Revision 4, requires that the IT security controls of each system be assessed on a continuous basis. OPM's Continuous Monitoring Strategy establishes objectives of the Information Security Continuous Monitoring (ISCM) program, activities that must be executed to meet those objectives, and roles and responsibilities to ensure successful completion of those activities.

OPM's OCIO has developed an ISCM Plan that includes a template outlining the security controls that must be tested for all information systems. All SOs are required to tailor the ISCM 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 quarterly basis for centralized tracking.

While the guidance established by OPM appears to be adequate, our review indicates that the continuous monitoring submission process is consistent with our findings in FISMA. We found three systems within the scope of this audit that did not perform Quarter 4 FY 2019 testing. The security control assessor did not complete the Continuous Monitoring Security Report in accordance with OPM's continuous monitoring strategy.

The security control assessor did not complete the Continuous Monitoring Security Report in accordance with OPM's continuous monitoring strategy.

OPM s Continuous Monitoring Policy states that the security control assessor is responsible for monitoring and auditing privacy controls in accordance with the continuous monitoring strategy. This includes completing the Continuous Monitoring Security Report on a quarterly basis.

Failure to adhere to the continuous monitoring strategy increases the risk that information about vulnerabilities and threats will not be available to support organizational risk management decisions.

This finding is consistent with the open recommendation in the FY 2019 FISMA audit report (Report No. 4A-CI-00-19-029, Recommendation 41) that recommends that OPM ensures that an annual test of security controls has been completed for all systems.

I. 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.

We do not believe that OPM has an effective Contingency Planning program.

We do not believe that OPM has an effective Contingency Planning program. Our findings are documented below.

1. Contingency Plan

OPM developed its contingency planning policy based on NIST, OMB, and FIPS guidance. OPM s Contingency Planning Policy states that contingency plans must be reviewed annually. OPM's Security Authorization Guide states, "The ISSO works with the SO to complete the [contingency plan]." OPM's contingency plan (CP) template was created using guidance from NIST SP 800-34, Revision 1. The template provides instructions and placeholders for the SO and ISSO to update with relevant system information.

We reviewed the CP and Business Impact Analysis (BIA) for the 15 systems in our audit scope. While most of the contingency plans were complete, we made the following observations:

- The BIA for two systems contains multiple, conflicting values for the recovery time objective;
- The BIA for SBM contains a recovery time objective value that is larger than the maximum tolerable downtime value;
- Three of the CPs contain a security categorization for the system that conflicts with the FIPS 199 security categorization;
- One CP contains a recovery time objective value that conflicts with the recovery time objective value determined in the BIA; and
- Three CPs are not dated within the last year and lack evidence of an annual review.

The SO is not completing a sufficiently detailed review of contingency planning documents at the agency defined frequency or in the event of a system change to ensure the accuracy of information and compliance with contingency planning controls.

NIST SP 800-53 Revision 4, states that the SO "Reviews the contingency plan for the information system [Assignment: organization-defined frequency] … ." NIST SP 800-53, Revision 4, also states that the SO will update "the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing … ."

Failure to review and update the contingency plan can have a negative impact on OPM's ability to respond to system availability incidents in an effective and timely manner.

Recommendation 7

We recommend that OPM implement a contingency plan review process to ensure the accuracy of information and compliance with contingency planning controls.

OPM Response:

"We concur. Ultimately, the contingency plan review is the responsibility of the System Owner (SO). Our OCIO team does provide the prompts, support and a documented process for the System Owner to conduct the review. We will further incorporate the SOs in the development of documentation and ensure they are aware of the resources available on the publication site in order to support closure of the recommendation."

2. Business Impact Analysis

OPM's Contingency Planning policy states that it is the responsibility of the SO to "Conduct a business impact analysis for the information system, in coordination with the business sponsor, to identify essential missions and business functions and associated contingency requirements." OPM developed a BIA worksheet using guidance from NIST SP 800-34, Revision 1. They also developed a BIA procedure document to assist the SOs to accurately define how their system impacts primary mission essential functions. At a minimum, a BIA is to be completed every three years.

We believe that OPM's BIA process is effective as the majority of the systems in our scope had a valid BIA.

We believe that OPM's BIA process is effective as the majority of the systems in our scope had a valid BIA. However, two of the system BIAs were performed by a contractor. The contractor performed the BIA based on its business process as it relates to its mission. OPM has not identified the business processes that are supported by the information system as it relates to the agency. The analysis performed by the contractor does not mention OPM nor the impact of the system on the agency.

NIST SP 800-34, Revision 1, guidance states that the contingency plan coordinator "should work with management and internal and external points of contact … to identify and validate mission/business processes and processes that depend on or support the information system" and work "with the process owners, leadership and business managers [to] determine the acceptable downtime if a given system were disrupted or otherwise unavailable."

Third-party contractors did not define the business needs of OPM. OPM should diagnose the impact of a system outage and reasonable downtimes for its business processes.

Recommendation 8

We recommend that OPM develop and implement a process that ensures SOs of contractor-operated systems work with internal process owners, leadership and business managers to create an OPM BIA.

OPM Response:

"We concur. We believe that processes should be in place and consistently implemented for both OPM and contractor operated systems. There is currently a process in place but was not implemented during the procurement of the services outlined for this recommendation. The OCIO is now retroactively evaluating and rectifying this."

3. Contingency Plan Testing

CP testing is a critical element of a viable disaster recovery capability. OPM requires that CPs 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 CPs and documenting the results. OPM does not have a template for CP testing so it is up to the SO to define what to test and what information to report in the test's after action report.

During the FY 2019 FISMA audit, we identified that CP testing was not performed annually for all OPM systems. Our current audit work shows that this issue still persists. CP tests were not completed within the last year for 5 of the 15 systems we assessed. The SOs did not coordinate a CP test within the last year.

NIST SP 800-53 Revision 4, states, "The organization … tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan." OPM's Contingency Planning Policy states that contingency plans must be tested at least annually.

Failure to test a CP increases the risk that the program office will not be effective in recovering systems in the event of an unplanned outage.

This finding is consistent with the open recommendation in the FY 2019 FISMA audit report (Report No. 4A-CI-00-19-029, Recommendation 47) that recommends that OPM test the contingency plans for each system on an annual basis.

Additionally, we observed three systems that did not have the sufficient scope appropriate for the security categorization of the system. All three systems only performed table-top CP tests. Moderate-impact systems should have performed a functional CP test while high-impact systems require a full-scale CP test.

OPM s Contingency Planning Policy includes test, training, and exercise guidance from NIST SP 800-84. The policy states that contingency plans for high-impact systems must, at a minimum, undergo full-scale CP testing; moderate-impact systems must, at a minimum, undergo functional CP testing; and low-impact systems must, at a minimum, undergo table-top CP testing.

Failure to test a contingency plan with the appropriate scope increases the risk that the plan will not work in the event of a real availability incident.

Recommendation 9

We recommend that OPM adhere to the guidance in its Contingency Planning Policy and conduct full-scale tests for high-impact systems, functional tests for moderate-impact systems, and table-top tests for low-impact systems annually.

OPM Response:

"We concur. The OCIO does not currently have the resources to plan and conduct the full-scale, function and table-top tests and will identify the necessary resources and include this data in future budget submissions."

J. 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.

While OPM has adequate policies and procedures in place for its POA&M process, ISSOs are not effectively updating POA&Ms with adequate information.

While OPM has adequate policies and procedures in place for its POA&M process, ISSOs are not effectively updating POA&Ms with adequate information. Of the 361 POA&Ms reviewed, 109 were still in an initial or draft status more than six months after the creation date. Initial and

draft POA&Ms did not yet contain all of the information required (e.g., milestones, estimated completion dates, estimated costs and labor) for managing POA&Ms and remediating weaknesses cost effectively.

The OPM Security Authorization Guide states, "The ISSO is responsible for creating the initial POA&M based on the [risk assessment report] and [the risk assessment table]. The SO is responsible for updating the POA&M with resources required, appropriate milestones, and expected completion dates." OPM also developed a POA&M Guide to provide a standardized process to identify, document, manage, and remediate weaknesses for OPM security officials.

OPM's POA&M Guide states, "The ISSO and SO will work together to capture all of the data elements needed for accurate tracking, management, and reporting of the status of the remediation of the weakness. These elements include the necessary milestones, expected completion dates, required resources, and source of funding, which will then be captured in the POA&M repository by the ISSO."

The guide also lays out the update process: "The POA&M is updated by the ISSO on a continuous basis as new weaknesses are identified and progress is made to mitigate previously identified weaknesses."

The ISSO and SO are responsible for documenting the necessary information for the remediation of the weakness that created the POA&M. However, there are no established timeliness metrics for moving a POA&M from initial to draft and from draft to open.

Failure to properly document POA&Ms increases the risk that the agency will have the necessary information to address risks in a cost effective and efficient manner.

Recommendation 10

We recommend that OPM document the required milestone information so that the identified POA&Ms can be moved to an open status.

OPM Response:

"We concur. We have begun implementing improvements to the POA&M process, including tracking timeliness of POA&M stages and updated milestone details. Though we face ISSO resource constraints, as of the date of this response, we have considerably improved our metrics in this area. We plan to provide OIG and IOC [Internal Oversight and Compliance] with updated information for closure consideration in FY 2021 and would be happy to discuss and share current documentation as IOC and OIG are interested."

Recommendation 11

We recommend that OPM update its POA&M procedures to include timeliness metrics related to transitioning a POA&M from initial/draft status to open.

OPM Response:

"We concur. We have begun implementing improvements to the POA&M process, including tracking timeliness of POA&M stages and updated milestone details. Though we face ISSO resource constraints as of the date of this response, we have considerably improved our metrics in this area. We plan to provide OIG and IOC with updated information for closure consideration early in FY 2021 and would be happy to discuss and share current documentation as IOC and OIG are interested."

K. PRIOR AUDIT RECOMMENDATIONS

In FY 2017, we conducted an audit of OPM's Authorization methodology by primarily assessing OPM's main general support system, the LAN/WAN. We also performed an analysis of the completeness of the other Authorization packages within OPM's system inventory. We determined that there were several issues with the LAN/WAN Authorization package and issued four findings/recommendations.

Since the prior audit, OPM determined that the LAN/WAN system was too complex and dynamic to be managed as a single system. In an effort to improve the ability to manage the LAN/WAN, OPM began the process of sorting the system into five subcomponents.

As part of this audit we assessed OPM's progress towards implementing the recommendations of the prior audit by looking at three of the five subcomponent systems: Infrastructure and Networking Tools (I&N Tools), Endpoint Services, and Cyber General Support System (Cyber GSS). The following sections detail our review.

1. System Security Plan

During the prior audit, we observed that the LAN/WAN SSP did not include the critical system information or address all of the system's relevant security controls. The issues with the SSP carried forward into the independent security control testing of the system. The independent third party assessment had scope limitations, an incomplete SSP and assessment boundary, and a very limited testing window. Specifically, we found that the SSP:

- Did not adequately define the system environment;

- Did not fully and accurately identify all of the security controls applicable to the system; and

- Did not provide evidence that common or inherited controls were actually in place.

Our review of the component SSPs did not find any issues with system environment or inherited and common security controls. However, we identified issues with the security control selection.

The I&N Tools and Endpoint Services SSPs do not accurately identify all of the security controls applicable to the system. There were also several controls missing from the master control set. NIST SP 800-30, Revision 1, requires that specific controls be in place for all systems based on their security categorization.

Failure to document all applicable security controls in the SSP increases the risk to the system from both an implementation and testing perspective. We would like to see the issues above corrected as well as a signed SSP for the other component systems.

This finding is consistent with the open recommendation in the FY 2017 Authorization audit report (Report No. 4A-CI-00-17-014, Recommendation 1) that recommends OCIO complete an SSP for the LAN/WAN that includes all of the required elements from OPM's SSP template and relevant NIST guidance.

2. Security Controls Assessment

A key element to the Authorization process is a thorough testing of the system's security controls. OPM hired an independent third party to test the effectiveness of the security controls of the three component systems. We identified several issues with the security control testing:

- Incorrect Scoping – Both Endpoint Services and I&N Tools did not have all controls assessed by the independent assessor. Although the assessment plan scoped out Agency common controls, they did not assess all of the other required MODERATE or HIGH controls, respectively.

- Incorrect Risk Assessment Table – I&N Tools, Endpoint Services and Cyber GSS had controls that were identified as partially satisfied or not satisfied as part of the independent assessment but did not all properly move to the risk assessment table.

Of the 345 I&N Tools security controls that are required to be tested for a HIGH system, 44 controls weren't assessed. The Endpoint Services assessor failed to test 84 moderate controls. Evidence of missing controls during the assessment coincide with the errors found in the prior audit of the LAN/WAN.

The impact of these issues is that there is a significant risk that the security controls testing performed as part of their Authorization process did not identify security vulnerabilities that could have been detected with an appropriately thorough test. The test work does not meet the minimum requirements of a complete security controls assessment.

This finding is consistent with the open recommendation in the FY 2017 Authorization audit report (Report No. 4A-CI-00-17-014, Recommendation 2) that recommends OCIO perform a thorough security controls assessment on the LAN/WAN. This assessment should address the deficiencies listed in the section above, and should be completed after a current and complete SSP is in place.

3. **Plan of Action and Milestones**

During the FY 2017 Authorization audit, OPM was unable to provide a list of POA&Ms from the assessment performed on the LAN/WAN during the Authorization Sprint. The LAN/WAN risk assessment identified 66 weaknesses. OPM provided a list in response to the draft report, but the POA&M list did not contain 51 of the 66 expected POA&Ms. OPM has not closed this recommendation and with the plan to decommission LAN/WAN in favor of the component systems, we would like to see each of the five component systems maintain an accurate POA&M list.

OPM has drafted POA&Ms for I&N Tools, Cyber GSS, and Endpoint Services. The POA&Ms are not in an open status as OPM is still in the process of authorizing the LAN/WAN component systems.

Failure to document remediation plans for weaknesses identified in Authorizations inhibits the ability to understand the scale of a system's security risk or allocate the appropriate resources to remediate weaknesses in a timely manner.

This finding is consistent with the open recommendation in the FY 2017 Authorization audit report (Report No. 4A-CI-00-17-014, Recommendation 3) that recommends that the OCIO update and maintain a complete POA&M list for the LAN/WAN.

4. Other Authorization Packages

During the FY 2017 audit, we determined that 13 of the Authorization packages completed during the Authorization Sprint were not completed appropriately. Those packages had insufficient SSP supporting documentation, incomplete security control assessments, and/or missing POA&Ms.

OPM has provided the missing elements for seven of the systems with documentation weaknesses and has decommissioned three systems. However, there are still three systems with incomplete or missing documentation identified during the Authorization Sprint.

This finding is consistent with the open recommendation in the FY 2017 Authorization audit report (Report No. 4A-CI-00-17-014, Recommendation 4) that recommends OCIO perform a gap analysis to determine what critical elements are missing and/or incomplete for all Authorization packages developed during the Sprint. For systems that reside on the LAN/WAN general support system, the OCIO should also evaluate the impact that an updated LAN/WAN SSP has on these systems' security controls.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

August 4, 2020

MEMORANDUM FOR: Chief, Information Systems Audits Group

FROM: Clare A. Martorana
Chief Information Officer

SUBJECT: & Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology (Report No. 4A-CI-00-20-009)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology, Report Number 4A-CI-00-20-009.

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

Recommendation 1: We recommend that OPM perform a full assessment for SBM and update all Authorization documentation in accordance with NIST guidance.

Management Response: We concur that a full assessment must be conducted. The OCIO will coordinate with supported business offices to obtain the resources needed to conduct the assessment and update appropriate documentation.

Recommendation 2: We recommend that OPM update its policies and procedures to include guidance on categorizing HVA systems.

Management Response: We do not concur. OPM implemented its current security categorization process and template based on the Office of Management and Budget (OMB) memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. The first objective in this memorandum includes the identification of High Value Assets (HVAs). Although the Federal Information Processing Standard (FIPS) 199 is referenced in the memorandum, the process for identification of HVAs and the security

categorization process are distinct. Each process has its own set of requirements and it is known by the Federal cybersecurity community that having a system go through the HVA identification process and come out as an HVA does not mean that the system will be identified as a High impact system using the FIPS 199 process. When OPM built its template, it was at the forefront of blending the two. The intent was to have the information in one location; however, at no point are processes for identifying HVA and High impact systems conjoined. The HVA worksheet template, as designed by the OPM OCIO, has not been used incorrectly from the intended purpose and has not led to the incorrect categorization of an OPM system.

Recommendation 3: We recommend that OPM have the SO, the CISO, the AO, and (where appropriate) the Chief Privacy Officer review and approve the categorization of the systems in its inventory, in accordance with agency policy.

Management Response: We concur. The work conducted in this area has led to security categorizations signed in accordance with OPM policies and procedures for the vast majority of the major systems within its inventory. The OCIO will coordinate with OPM offices to collect the signatures necessary in accordance with its policies and procedures.

Recommendation 4: We recommend that OPM develop and implement a process to perform annual quality reviews for SSPs. The process should include the elements defined in NIST SP 800-18, Revision 1.

Management Response: We concur. We will finalize documentation in the form of a Standard Operating Procedure (SOP) to ensure the annual review occurs consistently. Please refer to the provided technical comments.

Recommendation 5: We recommend that OPM routinely ensure that all SSP master control sets are updated with POA&M references.

Management Response: We do not concur. The OIG states, "If planned controls are not properly identified by the ISSO, an incomplete master control set can lead to the AO accepting unidentified risks and leave OPM vulnerable to potential exploits."

However, the System Security Plan (SSP) is not used as a document to communicate risk to the Authorizing Official. OPM uses other materials, including the Risk Assessment Table (RAT), Risk Assessment Report (RAR), Plan of Action and Milestones (POA&M), and a recommendation letter to provide applicable risk information to the Authorizing Official in order for the official to make an authorization decision. When an Authorizing Official review and makes a risk determination and authorization, the SSP and a POA&M line item would not lead to

"… the AO accepting unidentified risks and leave OPM vulnerable to potential exploits." The Authorizing Official is provided a complete set of materials before making such decisions.

Recommendation 6: We recommend that OPM improve the training program for new and current ISSOs on OPM's Authorization process. Training should include guidance on how to provide proper oversight related to security control scoping and risk identification and documentation.

Management Response: We concur. OPM agrees with the OIG position on this recommendation and we have identified strategic hiring needs within the ISSO role and other positions that contribute to these functions. OPM will update the guidance provided in its training for ISSOs upon obtaining the necessary resources.

Recommendation 7: We recommend that OPM implement a contingency plan review process to ensure the accuracy of information and compliance with contingency planning controls.

Management Response: We concur. Ultimately, the contingency plan review is the responsibility of the System Owner (SO). Our OCIO team does provide the prompts, support and a documented process for the System Owner to conduct the review. We will further incorporate the SOs in the development of documentation and ensure they are aware of the resources available on the publication site in order to support closure of the recommendation.

Recommendation 8: We recommend that OPM develop and implement a process that ensures SOs of contractor-operated systems work with internal process owners, leadership and business managers to create an OPM BIA.

Management Response: We concur. We believe that processes should be in place and consistently implemented for both OPM and contractor operated systems. There is currently a process in place but was not implemented during the procurement of the services outlined for this recommendation. The OCIO is now retroactively evaluating and rectifying this.

Recommendation 9: We recommend that OPM adhere to the guidance in its Contingency Planning Policy and conduct full-scale tests for high-impact systems, functional tests for moderate-impact systems, and table-top tests for low-impact systems annually.

Management Response: We concur. The OCIO does not currently have the resources to plan and conduct the full-scale, function and table-top tests and will identify the necessary resources and include this data in future budget submissions.

Recommendation 10: We recommend that OPM document the required milestone information so that the identified POA&Ms can be moved to an open status.

Management Response: We concur. We have begun implementing improvements to the POA&M process, including tracking timeliness of POA&M stages and updated milestone details. Though we face ISSO resource constraints, as of the date of this response, we have considerably improved our metrics in this area. We plan to provide OIG and IOC with updated information for closure consideration in FY 2021 and would be happy to discuss and share current documentation as IOC and OIG are interested.

Recommendation 11: We recommend that OPM update its POA&M procedures to include timeliness metrics related to transiting a POA&M from initial/draft status to open.

Management Response: We concur. We have begun implementing improvements to the POA&M process, including tracking timeliness of POA&M stages and updated milestone details. Though we face ISSO resource constraints as of the date of this response, we have considerably improved our metrics in this area. We plan to provide OIG and IOC with updated information for closure consideration early in FY 2021 and would be happy to discuss and share current documentation as IOC and OIG are interested.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Darrin McConnell, (202) 606-6210, and Darrin.McConnell@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