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-00-17-014
June 20, 2017

EXECUTIVE SUMMARY

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

Report No. 4A-CI-00-17-014 **June 20, 2017**

Why Did We Conduct the Audit?

Since fiscal year (FY) 2014, the number of U.S. Office of Personnel Management (OPM) information systems without a current and valid Security Assessment and Authorization (Authorization) was significant enough to warrant reinstating a material weakness related to this issue. In FY 2015, OPM placed a moratorium on all Authorization activity, further weakening the agency's security posture.

In FY 2016, OPM initiated an "Authorization Sprint" (Sprint) in an effort to get all of the agency's systems compliant with the Authorization requirements. We performed this audit to evaluate OPM's progress in addressing the material weakness.

What Did We Audit?

Our objectives were to review OPM's current Authorization methodology and to evaluate the Authorization packages completed during the Sprint. We focused our efforts on reviewing the Authorization package for OPM's primary general support system, the Local Area Network / Wide Area Network (LAN/WAN).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

OPM has dedicated significant resources toward re-Authorizing the systems that were neglected as a result of the 2015 Authorization moratorium. Although the program has notably improved, the deficit left by the moratorium continues to hamper the agency. We detected significant problems with the Authorization packages prepared during the Sprint, and there is still significant effort needed to stabilize the Authorization program. Of primary concern is the fact that the assessors performing the Sprint activity did not have access to enough accurate and complete information to make valid risk-based decisions about the systems' security posture. Our specific concerns include:

- The LAN/WAN system security plan (SSP) was missing relevant data about hardware, software, minor systems, and inherited controls. Additionally, the LAN/WAN SSP also failed to appropriately address several relevant controls, labeled as "not applicable."

- Deficiencies in the security control testing performed as part of the LAN/WAN Authorization process likely prevented the assessors from identifying security vulnerabilities that could have been detected with an appropriately thorough test.

- The security weaknesses detected during the LAN/WAN Authorization were not appropriately tracked in a Plan of Action and Milestones document.

- Critical elements were missing from many of the other Authorization packages prepared during the Sprint.

OPM has acknowledged the deficiencies of the Sprint Authorization packages, and explained that its intent was to obtain an initial level of compliance with Authorization requirements. It has already initiated a secondary review of the LAN/WAN Authorization in order to address said deficiencies, and we will monitor this effort closely. However, at this time, we continue to believe that OPM's management of system Authorizations represents a material weakness in the internal control structure of the agency's IT security program.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
LAN/WAN	**Local Area Network / Wide Area Network General Support System**
IG	**Inspector General**
IOC	**Internal Oversight and Compliance**
IT	**Information Technology**
NIST	**National Institute of Science and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
POA&M	**Plan of Action and Milestones**
SP	**Special Publication**
Sprint	**"Authorization Sprint"**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act. It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior Act. As part of our evaluation, we reviewed the U.S. Office of Personnel Management (OPM)'s FISMA compliance strategy and documented the status of their compliance efforts. In accordance with FISMA, this final report details the findings, conclusions, and recommendations resulting from an audit specific to OPM's controls over its Security Assessment and Authorization (Authorization) methodology.

An information system 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 risk associated with the system is deemed to be acceptable, then the system is formally authorized to operate in the agency's production information technology (IT) environment.

Our fiscal year (FY) 2010 FISMA report identified a material weakness in OPM's Authorization program related to incomplete, inconsistent, and sub-par Authorization products. OPM resolved these initial issues by implementing new policies and procedures to standardize the Authorization process. However, throughout FY 2014 and FY 2015, the number of OPM systems that had not been subject to the Authorization process significantly increased, and we reinstated the material weakness related to this issue.

In April 2015, OPM's Office of the Chief Information Officer (OCIO) issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through the end of FY 2016. In effect, all Authorization activity at OPM was halted. The OCIO's justification was that the agency was in the process of migrating its IT infrastructure to two new data centers and modernizing all of its applications, and that once this effort was completed, all systems would have to receive new Authorizations anyway. We expressed serious concern with this approach, and warned the agency of the extreme risk associated with neglecting the IT security controls of its information systems.

Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on the agency. The original modernization and migration effort was scrapped, and the agency is taking a different approach. As a result, many of the systems included in the memorandum operated in the same legacy environment without a valid Authorization.

OPM is also working to implement a comprehensive security control continuous monitoring program that will eventually replace the need for periodic system Authorizations. Although the agency's continuous monitoring program is rapidly improving, it has not reached the point of maturity where it can effectively replace the Authorization program. In addition, OPM acknowledges that a current and comprehensive Authorization for each system is a prerequisite for a continuous monitoring program, as the Authorization will provide a baseline of the security controls that need to be continuously monitored going forward.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objectives were to review OPM's Authorization methodology and to evaluate all of the completed Authorization packages against OMB, FISMA, and National Institute of Science and Technology (NIST) regulations, as well as OPM's own policies and procedures.

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, we obtained an understanding of OPM's Authorization process through inspection of various documents, including IT and other related organizational policies and procedures.

The scope of this audit included a review of OPM's 28 recently completed Authorization packages, including the Authorization for the Local Area Network / Wide Area Network general support system (LAN/WAN). The LAN/WAN is OPM's most critical general support system, as it provides inheritable controls to many of the agency's major information systems and smaller applications.

NIST Special Publication (SP) 800-37 identifies the key documents that an Authorization package should contain:

(i) the security plan;

(ii) the security assessment report; and

(iii) the plan of action and milestones (POA&M).

Using a risk based approach we selected the LAN/WAN as the focal point for our review since many of the other major systems at OPM reside on and inherit controls from this general support system.

To accomplish our objective, we reviewed federal laws, OMB policies and guidance, NIST guidance, OPM IT policies and procedures, and relevant Authorization documentation.

The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at OPM as of March 2017 and 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. These criteria include, but are not limited to, the following publications:

- OPM Information Security and Privacy Policy Handbook;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and

- Other criteria as appropriate.

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

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from December 2016 through March 2017 in OPM's Washington, D.C. office.

We discussed the results of our audit with OCIO representatives at an exit conference.

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

The following sections detail the results from our review of OPM's Authorization methodology.

A. AUTHORIZATION SPRINT

In an effort to revitalize its Authorization program, in FY 2016 OPM initiated an "Authorization Sprint" (Sprint) designed to get all of the agency's systems compliant with the Authorization requirements. OPM dedicated significant resources toward re-Authorizing the systems that were neglected as a result of the 2015 Authorization moratorium. This Sprint was originally intended to be a concentrated 30-day effort involving the expedited review and Authorization of systems. However, OPM has since continued its efforts to improve its Authorization compliance. In tandem, OPM has also been updating the templates and guidance that support the Authorization process. Since the start of the Sprint, OPM has performed Authorization work on all 28 systems whose Authorization had expired during or prior to this time period.

Although the program has notably improved, the deficit left by the moratorium continues to hamper the agency. As detailed in the sections below, we detected significant problems with the Authorization packages prepared during the Sprint, and there is still an enormous amount of effort needed to stabilize the Authorization program. Of primary concern is the fact that the assessors performing the Sprint activity did not have access to enough accurate and complete information to make valid risk-based decisions about the systems' security posture.

We acknowledge that the lack of a valid Authorization does not necessarily mean that a system is insecure. However, it does mean that a system is at a significantly higher risk of containing unidentified security vulnerabilities. A thorough Authorization process almost always identifies significant issues that must be addressed. If the process was not properly followed, then the agency does not know what weaknesses and vulnerabilities exist in its IT environment, and it cannot take steps to address and remove those weaknesses.

OPM's management of system Authorizations continues to represent a material weakness.

At this time, we continue to believe that OPM's management of system Authorizations represents a material weakness in the internal control structure of the agency's IT security program[1]. It is our understanding that the agency acknowledges this weakness and has a plan in place to address it, and we will continue to monitor this activity closely.

[1] OPM OIG Audit Report No. 4A-CI-00-16-039, Recommendation 4, recommends that all systems in OPM's inventory have a complete and current Authorization, and labels this issue as a material weakness. The results of this current audit determined that the material weakness and the associated audit recommendation both remain open.

B. SECURITY AUTHORIZATION GUIDE

In 2016, the OCIO made several improvements to the OPM Authorization process. These included:

- Establishing and documenting a new Security Authorization Guide based on NIST's risk management framework;
- Updating the roles and responsibilities for individuals in the Authorization process; and
- Updating outdated templates for the various Authorization elements.

Nothing came to our attention to indicate that the OCIO has not developed an adequate framework surrounding the Authorization process. OPM should continue to apply this new framework as it works to improve its Authorization program.

C. LAN/WAN GENERAL SUPPORT SYSTEM AUTHORIZATION

The OPM LAN/WAN was approved to continue operating in a production environment on September 12, 2016. At that time, the OCIO acknowledged issues with the Authorization package and therefore only approved the Authorization to be valid for one year (instead of the traditional three years).

As described below, the LAN/WAN system security plan (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 assessor's test work was restricted by missing information, inappropriate scope limitations, and insufficient time to assess a general support system of this size.

Considering that the LAN/WAN is the agency's primary general support system and hosts many of OPM's other major applications, the issues found in the LAN/WAN Authorization have a significant impact to the security of OPM as a whole.

The following sections detail our review of the LAN/WAN Authorization package.

1) System Security Plan

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

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

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

Our review of the LAN/WAN SSP identified several gaps between the documentation provided and the relevant guidance and policies including:

System Environment

The LAN/WAN SSP did not adequately define the system environment, as it did not contain complete hardware, software, or minor system inventories.

According to OPM's SSP Template, "The purpose of [system security planning] is to . . . describe the controls and critical elements in place . . . ." We do not believe that the LAN/WAN SSP meets this objective because it does not define the boundaries of the general support system. Without complete inventories, the system owner does not have the information necessary to design controls that protect the entire environment, and an independent assessor cannot effectively evaluate the security posture of the system as a whole.

Security Control Selection

The LAN/WAN SSP does not fully and accurately identify all of the security controls applicable to this system. Specifically, the LAN/WAN SSP inappropriately identified multiple controls as "not applicable," but NIST guidelines require these specific controls to be in place for all systems with a HIGH security categorization (such as the LAN/WAN.)

Failure to document all applicable security controls in the SSP increases the risk to the system from both an implementation and testing perspective. If the SSP identifies a control as "not applicable," a system owner is less likely to implement the control, and an assessor would likely exclude it from the scope of its testing.

Inherited and Common Security Controls

A substantial number of controls are identified as "common" or "inherited" by the LAN/WAN, but the SSP does not provide evidence that these controls are actually in place. NIST 800-37, Revision 1, requires that common control providers operate effectively as an independent system, requiring security planning, security assessment reporting, POA&M tracking, and continuous monitoring. Failure to maintain evidence that common or inherited controls are in place and operating as designed increases the risk that the LAN/WAN and the applications hosted by this support system contain unidentified vulnerabilities.

Recommendation 1

We recommend that the OCIO complete an SSP for the LAN/WAN that includes all of the required elements from OPM's SSP template and relevant NIST guidance. This includes, but is not limited to, the specific deficiencies outlined in the section above.

OPM Response:

"OPM concurs with the recommendation. During the course of the assessment, the LAN/WAN SSP was being modified to incorporate components that were a part of the infrastructure data centers that were being 'stood up' as a part of the infrastructure improvement program. The system environment was also being modified as a result of two other infrastructure system boundaries being merged into the LAN/WAN system boundary as separate subsystems. This resulted in a complex, dynamic system that made it difficult for the

OPM recognized the deficiencies of the LAN/WAN SSP and proactively initiated a review and update of this document.

independent assessor to evaluate the status of many security controls with a high degree of confidence. Understanding this, OPM determined that a supplementary assessment would be needed to reevaluate those controls that were not fully successful during the initial assessment, once the environment has fully incorporated these changes. OPM believes that the environment has reached this state and OPM will provide an updated SSP for the LAN/WAN, which addresses the gaps identified by the OIG, as soon as it is available.

In regards to the OIG statement that the LAN/WAN SSP inappropriately identified multiple controls as 'not applicable,' OPM would like to provide clarification. NIST provides security control baselines for system owners to tailor and supplement in order to protect the information stored, processed, and transmitted by the system. Consistent with NIST 800-37, these controls are not specifically required until the controls go through the tailoring process. Any tailoring decisions must be documented and approved by the Authorizing Official (AO). The results of the tailoring process will be more readily apparent in the updated SSP, including a well-defined rationale for controls that are not applicable as previously identified by the OIG."

OIG Comment:

We acknowledge the complexities that OPM faced when assessing the security controls of the LAN/WAN environment at a time when its boundaries were in a state of fluctuation. However, these complexities do not negate the criticality of a comprehensive Authorization based on a complete and accurate SSP. We will continue to monitor OPM's efforts to update the LAN/WAN SSP as the environment approaches a more stable state.

We also acknowledge that the NIST SP 800-53 security controls must be tailored to each individual information system. However, it is not appropriate to simply list controls as "not applicable" without providing the relevant details to justify this conclusion, as it appears was done with the LAN/WAN SSP.

We continue to recommend that OCIO provide Internal Oversight and Compliance (IOC) with evidence that the revised SSP has addressed all of our concerns outlined above.

An updated version of the LAN/WAN SSP was provided to the OIG several weeks after the completion of the draft reporting phase of this audit. This document and any other artifacts completed after the draft reporting phase of the audit closed will be reviewed in the upcoming general FISMA audit.

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 LAN/WAN general support system. We identified several issues with the LAN/WAN security controls test:

- Scope limitations – Critical components of the LAN/WAN were intentionally excluded from the scope of the security controls test. Specifically, the test work did not include applications and software installed on the LAN/WAN servers. In addition, multiple physical facilities hosting the LAN/WAN hardware were excluded from testing.

- Incomplete SSP and boundary – As mentioned in the section above, there are flaws in the most recent LAN/WAN SSP that was submitted with the final Authorization package. However, no current SSP was available to the security assessment team at the time the LAN/WAN security controls were tested. Not only was the SSP provided to the assessors outdated by approximately one year, but as described by the assessors it "did not contain the level of detail required to accurately describe the system, the assessment boundary . . ., or determine the plan, intent, and implementation status of each control."

- Testing limitations – The assessment team was given a very limited window of seven days to perform the test work. This was not adequate time for the team to acquire the required evidence for controls that were simply described verbally in interviews. The assessor's report states "While the interview sessions were extremely informative, the required evidence was not collected and a number of the technical interview statements were not witnessed via shoulder surf or screen-share during the review process."

Of the 334 LAN/WAN security controls that were tested, 202 were either not satisfied or only partially satisfied. The assessment team also noted that "There were thousands of findings that were the result of scans and missing documentation but were rolled up where applicable to cut down on the number of actual results."

The cumulative impact of these issues is that there is a significant risk, if not likelihood, that the security controls testing performed as part of the LAN/WAN Authorization process did not identify security vulnerabilities that could have been detected with an

The LAN/WAN security controls assessment likely did not identify vulnerabilities that could have been detected with a thorough test.

appropriately thorough test. It is our opinion that this test work does not meet the minimum requirements of a complete security controls assessment.

As a result, the Authorization package as a whole likely under-represents the quantity and severity of security risks associated with this system. This risk is compounded by the fact that a substantial number of other OPM systems are designed to inherit security controls from the LAN/WAN.

Recommendation 2

We recommend that the 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 thorough SSP is in place (see Recommendation 1).

OPM Response:

"OPM concurs with the recommendation. OPM would like to provide clarification, however, to the OIG assertion that critical components of the LAN/WAN were intentionally excluded from the assessment. The Security Assessment Plan provides a statement of software that is excluded and software that is included. The exclusions identified in the Security Assessment Plan and the Security Assessment Report refer to application software that is included in the security authorization boundary of other systems. Consistent with NIST 800-53, these application boundaries were outside of the scope of the LAN/WAN assessment because they were covered by separate system assessments; thus it was not appropriate to include them in the LAN/WAN Security Assessment Plan. OPM is taking into consideration that the language in the Security Assessment Plan may be an area where OPM can clarify what it has done and why and thus improve its performance during the current assessment effort of the LAN/WAN and common controls.

OPM's General Comments and Response to Recommendation 1 also apply to the OIG statements concerning the SSP and boundary.

In the draft, OIG stated that an assessor made a statement to the effect that findings were rolled up to cut down on the number of actual results, which OPM believes is misleading and conveys inaccurate implications that OPM is compelled to correct. As a part of the assessment, the assessor is responsible for identifying the number of occurrences of a specific potential vulnerability. For the generation of the Plan of Action and Milestones

(POA&Ms), each instance of a potential risk that occurs in the environment is not reported separately; including the information separately would make the POAMs too detailed and cumbersome to be useable or effective. Rather, these instances are rolled up into higher-level POA&Ms for reporting and management. This practice comports with OMB policy of the generation of POA&Ms, and is followed by OPM and other Executive agencies."

OIG Comment:

We agree with OCIO's statement that application software installed on the servers do not require testing if they fall within the authorization boundaries of other systems. However, not all of the LAN/WAN's applications are within other system boundaries; OPM's security and network monitoring tools are prime examples. We believe these applications should not have been excluded from the assessment, as they are pertinent to the security and risk of all systems inheriting controls from the LAN/WAN. The LAN/WAN SAP also excludes several OPM data centers from testing and simply states that they will be tested on a later date due to a condensed timeline. As such, there is a likelihood that the testing performed as part of the LAN/WAN Authorization process did not identify security vulnerabilities that could have been detected with a complete and thorough test.

Regarding the number of weaknesses detected by the assessors, we agree with OPM that it is appropriate to roll multiple instances of the same finding into a single POA&M entry. Our reference to the number of controls that the assessor labeled as "not satisfied" is simply a reference to the magnitude of problems detected with the LAN/WAN's security controls.

3) Plan of Action and Milestones

A POA&M is a tool used to assist agencies in recording, 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.

A POA&M is typically used to track the security weaknesses identified during the Authorization process. However, OPM was unable to produce this documentation for the LAN/WAN.

The OPM Authorization Guide states "All risks that have not been remediated must be documented in the POA&M, including risks from controls inherited from other systems, risks from the independent assessment, and any predefined risks." The risks identified during the

Authorization process are added to any previously identified risks so that the POA&M list contains all known weaknesses and their remediation plans. NIST SP 800-53, Revision 4, states that an organization must develop "a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system . . . ."

Failure to document remediation plans for weaknesses identified in Authorizations inhibits the process of understanding the scale of a system's security risk and allocating the appropriate resources to remediate weaknesses in a timely manner.

Recommendation 3

We recommend that the OCIO update and maintain a complete POA&M list for the LAN/WAN.

OPM Response:

"OPM concurs with the recommendation. OPM provided the POA&M for the LAN/WAN after receiving the draft audit report, which should result in closure of this recommendation."

OIG Comment:

OPM did provide a POA&M list for the LAN/WAN as a part of its response to the draft report, but it did not contain all existing weaknesses identified during the LAN/WANs independent assessment (only 15 of the independent assessor's 66 findings were included). We continue to recommend that OCIO update and maintain the POA&M for all existing vulnerabilities and provide IOC evidence once this has been completed.

D. Other Authorization Packages

While this audit largely focused on the LAN/WAN Authorization, we also reviewed all Authorization packages performed during the Sprint. There were several issues that we detected across multiple packages, including:

- SSP supporting documentation – An SSP should include multiple appendices for important system information. These documents should address privacy considerations, security

classifications, system inventories, and contingency planning. A significant number of packages were missing various elements of supporting documentation.

- Security controls assessments – Many Authorization packages lacked evidence that the system was subject to a thorough security controls assessment.

- POA&Ms – A significant number of packages were missing a POA&M outlining the vulnerabilities detected during the assessment.

In short, many of the Authorization packages were not complete. We acknowledge that every OPM system has been technically "authorized to operate" by a senior-level official that has put their signature on a document stating that they accept all security risks associated with that system. However, we believe that the deficiencies in the Authorization packages completed as part of the Sprint prohibited these individuals from making a reasonably informed risk-based decision.

Many of the Authorization packages developed during the Sprint were not complete.

Recommendation 4

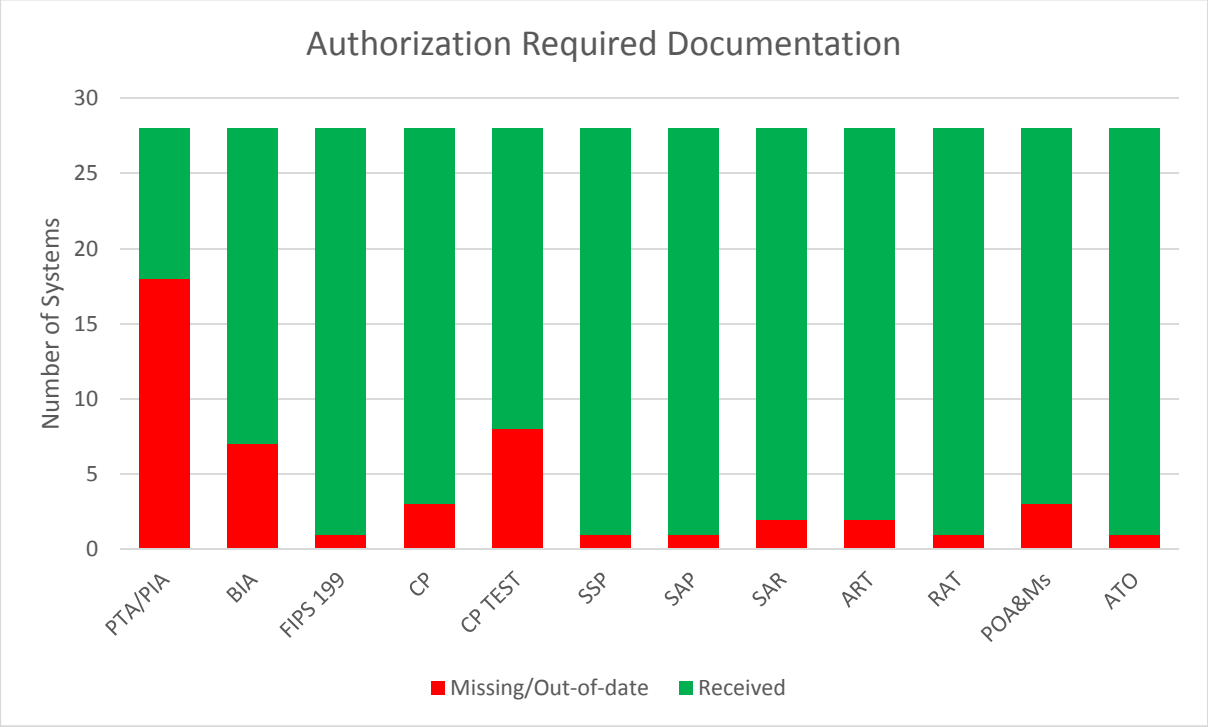
We recommend that the OCIO perform a gap analysis to determine what critical elements are missing and/or incomplete for all Authorization packages developed during the Sprint. For systems that reside on the LAN/WAN general support system, the OCIO should also evaluate the impact that an updated LAN/WAN SSP has on these systems' security controls.

OPM Response:

"OPM concurs with the recommendation and provides the following clarifications. OPM reviewed the gap analysis conducted by the OIG of the documents OIG identified as missing from authorization packages. OPM determined that some of the documents were included in the original set of evidence provided to OIG during the audit. OPM also provided several additional documents that OIG identified as missing from the packages. During the exit briefing, OPM updated the OIG on the status of its improvements to the automation of its system inventory and documentation repository. These improvements will support OPM's AOs to make risk determination and authorization decisions based on the status of controls inherited from its systems."

OIG Comment:

OPM provided us with multiple batches of Authorization documentation during and after the fieldwork phase of this audit. Our final review of all documentation provided by OPM determined that the Authorization packages completed during the Sprint continue to lack significant critical artifacts. We have still not received current and valid copies of 51 out of the 336 artifacts expected for the Authorization packages in the scope of this audit. The chart below provides a breakdown of missing documentation by artifact type.



While our review provides the OCIO with a head start in completing the gap analysis, it is the OCIO's responsibility to independently verify and update this information. The OCIO's analysis should also evaluate the impact that an updated LAN/WAN assessment has on the information systems that inherit security controls from the LAN/WAN. The owners of these other systems should be made aware of any deficiencies in the LAN/WAN's controls so that they can appropriately assess the risk to their own systems.

Once this process has been completed, the OCIO should provide IOC with the evidence that each system has a complete, up to date, Authorization package.

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF THE INSPECTOR GENERAL

FROM: DAVID L. DEVRIES
CHIEF INFORMATION OFFICER

DAVID DEVRIES
Digitally signed by DAVID DEVRIES
Date: 2017.04.06 16:35:32 -04'00'

Subject: Office of Personnel Management Response to the Office of the Inspector General Security Assessment and Authorization Methodology Audit (Report No. 4A-CI-00-17-014)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Security Assessment and Authorization Methodology for the U.S. Office of Personnel Management (OPM). The OIG comments are valuable to OPM as they afford us an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to OPM by the Federal workforce, the Federal agencies, private industry, and the public.

As noted in the OIG draft report, OPM initiated a project in Fiscal Year 2016 to update many of its Authorizations to Operate (ATOs) for its information systems. A rigorous and aggressive schedule was established to complete the project with a focus on the infrastructure that supports many of the other systems. During this time, OPM was making many changes to its network and notified its ATO assessors that they would be working in a highly dynamic environment; however, OPM believed that this important project should not be delayed. An assessment was conducted based on a snapshot of the inventory and environment at the time of the assessment. The assessor faced challenges in performing the assessment of this highly-dynamic environment. Therefore, the Authorizing Official for the infrastructure had to take both the highly dynamic environment, and the challenges the assessor faced in its assessment, into account when making the authorization decision. Due to the potential risk identified during the assessment, the ATO that was issued was for one year, instead of the three years typically authorized for an information system. Understanding the short duration of the ATO and the dynamic environment under which that ATO was assessed, OPM has already initiated a secondary assessment of the infrastructure to evaluate the security controls that were not fully satisfied from the initial assessment, including those where the assessor may have needed more time or evidence to evaluate. OPM is taking into consideration the recommendations provided in this report as it proceeds with this assessment.

We welcome a collaborative dialogue to help us fully understand the OIG's recommendations as we plan our remediation efforts so that our actions and the closure of the recommendations thoroughly address the underlying issues. We understand that the OIG may believe some system security packages are missing elements. We can provide supplementary documentation to address this; however, due to the time constraint governing this response, and some

confusion at the time of the document production portion of this audit, we acknowledge that such additional documentation has not yet been supplied as of the date of this response. And we stand ready to provide that documentation over the next several weeks, if that would be helpful. We have notified the OIG that we believe it is issuing the audit without the benefit of the full set of documentation available. We note below the areas where we believe additional information is necessary in order to place this Report's findings in the proper context. I look forward to continued discussions during our monthly reviews to help ensure we remain aligned.

Each of the recommendations provided in the draft report is discussed below:

Recommendation 1
We recommend that the OCIO complete a SSP for the LAN/WAN that includes all of the required elements from OPM's SSP template and relevant NIST guidance. This includes, but is not limited to, the specific deficiencies outlined in the section above.

OPM Response: OPM concurs with the recommendation. During the course of the assessment, the LAN/WAN SSP was being modified to incorporate components that were a part of the infrastructure data centers that were being "stood up" as a part of the infrastructure improvement program. The system environment was also being modified as a result of two other infrastructure system boundaries being merged into the LAN/WAN system boundary as separate subsystems. This resulted in a complex, dynamic system that made it difficult for the independent assessor to evaluate the status of many security controls with a high degree of confidence. Understanding this, OPM determined that a supplementary assessment would be needed to reevaluate those controls that were not fully successful during the initial assessment, once the environment has fully incorporated these changes. OPM believes that the environment has reached this state and OPM will provide an updated SSP for the LAN/WAN, which addresses the gaps identified by the OIG, as soon as it is available.

In regards to the OIG statement that the LAN/WAN SSP inappropriately identified multiple controls as "not applicable," OPM would like to provide clarification. NIST provides security control baselines for system owners to tailor and supplement in order to protect the information stored, processed, and transmitted by the system. Consistent with NIST 800-37, these controls are not specifically required until the controls go through the tailoring process. Any tailoring decisions must be documented and approved by the Authorizing Official (AO). The results of the tailoring process will be more readily apparent in the updated SSP, including a well-defined rationale for controls that are not applicable as previously identified by the OIG.

Recommendation 2
We recommend that the 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 thorough SSP is in place (see Recommendation 1).

OPM Response: OPM concurs with the recommendation. OPM would like to provide clarification, however, to the OIG assertion that critical components of the LAN/WAN were intentionally excluded from the assessment. The Security Assessment Plan provides a statement of software that is excluded and software that is included. The exclusions identified in the Security Assessment Plan and the Security Assessment Report refer to application software that

is included in the security authorization boundary of other systems. Consistent with NIST 800-53, these application boundaries were outside of the scope of the LAN/WAN assessment because they were covered by separate system assessments; thus it was not appropriate to include them in the LAN/WAN Security Assessment Plan. OPM is taking into consideration that the language in the Security Assessment Plan may be an area where OPM can clarify what it has done and why and thus improve its performance during the current assessment effort of the LAN/WAN and common controls.

OPM's General Comments and Response to Recommendation 1 also apply to the OIG statements concerning the SSP and boundary.

In the draft, OIG stated that an assessor made a statement to the effect that findings were rolled up to cut down on the number of actual results, which OPM believes is misleading and conveys inaccurate implications that OPM is compelled to correct. As a part of the assessment, the assessor is responsible for identifying the number of occurrences of a specific potential vulnerability. For the generation of the Plan of Action and Milestones (POA&Ms), each instance of a potential risk that occurs in the environment is not reported separately; including the information separately would make the POAMs too detailed and cumbersome to be useable or effective. Rather, these instances are rolled up into higher-level POA&Ms for reporting and management. This practice comports with OMB policy of the generation of POA&Ms, and is followed by OPM and other Executive agencies.

Recommendation 3
We recommend that the OCIO update and maintain a complete POA&M list for the LAN/WAN.

OPM Response: OPM concurs with the recommendation. OPM provided the POA&M for the LAN/WAN after receiving the draft audit report, which should result in closure of this recommendation.

Recommendation 4
We recommend that the 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.

OPM Response: OPM concurs with the recommendation and provides the following clarifications. OPM reviewed the gap analysis conducted by the OIG of the documents OIG identified as missing from authorization packages. OPM determined that some of the documents were included in the original set of evidence provided to OIG during the audit. OPM also provided several additional documents that OIG identified as missing from the packages. During the exit briefing, OPM updated the OIG on the status of its improvements to the automation of its system inventory and documentation repository. These improvements will support OPM's AOs to make risk determination and authorization decisions based on the status of controls inherited from its systems.

Again, thank you for the opportunity to provide comment. Please contact me or Mr. Cord Chase

if you have questions or need additional information.

cc:
Cord E. Chase
Chief Information Security Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

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