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

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S Local Area Network / Wide Area Network General Support System FY 2012

Report No. 4A-CI-00-12-014

Date: May 16, 2012

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S LOCAL AREA NETWORK / WIDE AREA NETWORK GENERAL SUPPORT SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-CI-00-12-014 **Date:** May 16, 2012

Michael R. Esser
Assistant Inspector General
for Audits

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S LOCAL AREA NETWORK / WIDE AREA NETWORK GENERAL SUPPORT SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-CI-00-12-014

Date: May 16, 2012

This final audit report discusses the results of our audit of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Local Area Network / Wide Area Network General Support System (LAN/WAN). Our conclusions are detailed in the "Results" section of this report.

Information System Security Plan (ISSP)

The LAN/WAN ISSP contains the majority of critical elements required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18. However, it fails to document minor controls owned by the OCIO and fails to identify external interconnections.

Certification and Accreditation Statement (C&A)

A C&A of the LAN/WAN was completed in June 2010. We reviewed the certification package for all required elements of a C&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199 Analysis

The security categorization of the LAN/WAN appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of "moderate."

Risk Assessment

A risk assessment was conducted for the LAN/WAN in May 2010 that addresses all the required elements outlined in relevant NIST guidance.

Independent Security Control Testing

A security control assessment was completed for the LAN/WAN as a part of the system's C&A process in May 2010.

Security Control Self-Assessment

The OCIO conducted a self-assessment of the security controls of the LAN/WAN in August 2011. However, a subset of controls for minor systems owned by the OCIO was not tested.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for the LAN/WAN that is in compliance with NIST SP 800-34 and is tested annually. However, the security categorization documented in the contingency plan is not consistent with the categorization in the FIPS 199 evaluation. The OCIO provided evidence to remediate this issue with the response to the draft audit report.

Privacy Impact Assessment (PIA)

A privacy threshold analysis (PTA) was conducted for the LAN/WAN. However, no PTAs have been conducted on the minor systems owned by the OCIO. Therefore, we do not know if a PIA is needed.

Plan of Action and Milestones (POA&M) Process

The LAN/WAN POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the OCIO for evaluation. However, the POA&M did not follow the color scheme established by the guide. The OCIO provided evidence to remediate this issue with the response to the draft audit report.

NIST SP 800-53 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 were implemented for LAN/WAN. Although the majority of the tested security controls have been successfully implemented, one control was not fully satisfied. User workstation settings related to unsuccessful login attempts do not comply with OPM's Information Security and Privacy Policy Handbook.

Contents

Introduction

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 (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the 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 accordance with FISMA, we audited the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Local Area Network / Wide Area Network (LAN/WAN) General Support System.

Background

The LAN/WAN is one of OPM's critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

As a hardware and software infrastructure environment, the LAN/WAN supports a variety of OPM information systems. OPM's Office of the Chief Information Officer (OCIO) is the organization responsible for the maintenance and operations of the LAN/WAN. The OCIO is also responsible for the software development and maintenance of some minor applications that reside on the general support system. The hardware supporting those systems is housed at OPM's Washington, D.C.; Macon, Georgia; and Boyers, Pennsylvania facilities.

This was our second audit of the security controls surrounding the LAN/WAN. All recommendations issued as part of the previous audit were closed prior to the start of this audit. We discussed the results of our audit with OCIO representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of the security controls for the LAN/WAN to ensure that OCIO officials have implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's OCIO.

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for the LAN/WAN, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;

- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of OCIO officials responsible for the LAN/WAN, including IT security controls in place as of January 2012.

We considered the LAN/WAN internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objective, we interviewed representatives of OPM's OCIO division and other individuals with OCIO security responsibilities. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of the LAN/WAN are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the LAN/WAN system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- OMB Circular A-130, Appendix 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 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 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;
- 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 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 November 2011 through January 2012 in OPM's Washington, D.C. office. This was our second audit of the security controls surrounding the LAN/WAN.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OCIO management of the LAN/WAN is consistent with applicable standards. Nothing came to our attention during this review to indicate that the OCIO is in violation of relevant laws and regulations.

Results

I. Information System Security Plan

Federal agencies must implement for each information system the security controls outlined in NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an Information System Security Plan (ISSP) for each system, and provides guidance for doing so.

The ISSP for the LAN/WAN was created using a template that is outlined in NIST SP 800-18. The ISSP contains the majority of the elements outlined by NIST. However, the ISSP does not document minor systems owned and operated by the LAN/WAN. Also, the ISSP does not contain details of the interconnections between the LAN/WAN and other systems.

a) Minor System Documentation

The OCIO owns and is responsible for the daily operation and security of a variety of minor applications that reside on the LAN/WAN. This list includes, but is not limited to, the email system, voice over IP telephone system, Blackberry servers, and the Remedy help desk tracking system. However, these systems are not documented in the LAN/WAN ISSP. The ISSP also does not discuss any security controls that are specific or unique to any of those systems.

NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, states that agencies must "ensure that the security requirements of minor applications are addressed as part of the system security plan for the applicable general support systems." The NIST guide also states that "security controls specific to the minor application should be documented in the system security plan as an appendix or paragraph."

Failure to appropriately document minor systems and the related security controls in the ISSP increases the risk that these systems are overlooked in the scope of the Authorization process and any subsequent security control testing.

Recommendation 1

We recommend that the OCIO document all minor applications and the security controls applicable to each one in the LAN/WAN ISSP.

OCIO Response:

"Network Management – Network Security (NM-NS) concurs with the OIG finding and Plan of Action and Milestones (POA&M) item FY12-Q2-LANWAN-287 was created and added to the Network Management – Network Security POA&M list."

OIG Reply:

As part of the audit resolution process, we recommend that OCIO provide Internal Oversight and Compliance (IOC) with evidence supporting the remediation of the recommendation.

b) External Interconnections

The LAN/WAN has interconnections with several systems owned by external entities. However, the details of these external interfaces are not disclosed in the ISSP as required by NIST SP 800-18. Specifically, the LAN/WAN ISSP does not detail the following information about each interfacing system: name, organization, type of interconnection, authorizations, dates of agreement, Federal Information Processing Standards (FIPS) 199 category, Certification and Accreditation (C&A) status, and name and title of authorizing official.

Recommendation 2

We recommend that the OCIO revise the LAN/WAN ISSP to include identifiers of the external systems that interconnect with the general support system (name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, and name and title of authorizing official).

OCIO Response:

"NM-NS concurs with the OIG finding and Plan of Action and Milestones (POA&M) item FY12-Q2-LANWAN-289 was created and added to the Network Management – Network Security POA&M list."

OIG Reply:

As part of the audit resolution process, we recommend that OCIO provide IOC with evidence supporting the remediation of the recommendation.

II. Certification and Accreditation Statement

A security C&A of the LAN/WAN was completed in June 2010.

OPM's IT Security Officer reviewed the LAN/WAN C&A package and signed the system's certification package on June 21, 2010. The system's owner signed the accreditation statement and authorized the continued operation of the system on June 16, 2010.

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements.

The OCIO's IT Security and Privacy group created and published guidance for preparing and conducting C&A's in April 2011. These policies and procedures are now in effect for all OPM systems. While the LAN/WAN C&A was appropriately conducted in accordance with the guidance available in 2010, we suggest that the system owners review OPM's new C&A

methodology and conduct a gap analysis to ensure that they are prepared to conduct their 2013 C&A in accordance with the new requirements.

Although the LAN/WAN C&A was generally conducted in compliance with NIST requirements, the LAN/WAN authorization to operate was signed by the system owner prior to the certification package being signed by the Chief Information Security Officer (CISO). The OPM Security Assessment and Authorization Guide states that "The CISO reviews the package and makes an overall assessment. The CISO then produces the authorization recommendation letter, which is attached to the package and forwards to the AO [Authorizing Official] for the final approval decision. The AO will issue an authorization decision (ATO, Denial of Authorization to Operate, or Limited Authorization to Operate) based on a review of the package, and the CISO recommendation." The OCIO should ensure that the guidelines set forth in the OPM Security Assessment and Authorization Guide are followed during the next LAN/WAN Authorization in 2013.

III. FIPS 199 Analysis

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The LAN/WAN ISSP categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The LAN/WAN is categorized with a moderate impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of moderate.

The security categorization of the LAN/WAN appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and we agree with the categorization of moderate.

IV. Risk Assessment

A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) results documentation.

A risk assessment was conducted for the LAN/WAN in May 2010 that adequately addresses the elements outlined in the NIST guidance.

V. Independent Security Control Testing

A security control assessment was completed for the LAN/WAN in May 2010 as a part of the system's C&A process. The security assessment was conducted by another government agency, the Federal Aviation Administration, which was operating independently from the OCIO. We reviewed the controls included in the scope of this test to ensure that they included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

The security assessment report labeled each security control as fully in place, partially in place, not in place, or not applicable. Nothing came to our attention to indicate that the security controls of the LAN/WAN have not been adequately tested by an independent source. However, as mentioned in section I above, minor applications have not been documented in the LAN/WAN ISSP, and therefore it is not possible to confirm that the scope of the independent testing included all minor applications operated by the OCIO. The OCIO needs to ensure that the minor systems owned and operated by the LAN/WAN are included in the scope of the next C&A and fully tested by an independent entity.

VI. Security Control Self-Assessment

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent security assessment is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

The OCIO conducted a self-assessment of the system in August 2011. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. However, there is no indication that the security controls of minor applications within the LAN/WAN are tested annually.

Recommendation 3

We recommend that the OICO test a subset of the security controls for minor systems annually as part of the self-assessment.

OCIO Response:

"NM-NS concurs with the OIG finding and has created POA&M item FY12-Q2-LANWAN-296 and added the item to the Network Management – Network Security POA&M list."

OIG Reply:

As part of the audit resolution process, we recommend that OCIO provide IOC with evidence supporting the remediation of the recommendation.

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for IT 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.

Contingency Plan

The LAN/WAN contingency plan documents the functions, operations, and resources necessary to restore and resume LAN/WAN operations when unexpected events or disasters occur. The LAN/WAN contingency plan closely follows the format outlined by NIST SP 800-34 and contains a majority of the suggested elements.

The scope of the LAN/WAN contingency plan indicates that it is classified as a high impact system. However, as mentioned above, the security categorization documented in the ISSP identifies the LAN/WAN as a "moderate" system. This inconsistency increases the risk that the scope of security control or contingency plan testing will be inappropriate.

Recommendation 4

We recommend that the OCIO review the contingency plan and the ISSP and address this inconsistency.

OCIO Response:

"NM-NS concurs with the OIG finding and has updated the LAN/WAN Information System Contingency Plan (ISCP). The document is enclosed with this memo."

OIG Reply:

We have reviewed the updated contingency plan for LAN/WAN and determined that it addresses the inconsistency related to the security categorization of LAN/WAN; no further action is required.

Contingency Plan Test

NIST SP 800-34, Contingency Planning Guide for Information Technology, provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

The OCIO participates in the annual Data Center disaster recovery test and also performs failover testing on Exchange 2007, Blackberry Enterprise System, Outlook Web Access, and agency file systems. The testing documentation includes the majority of elements suggested

by NIST SP 800-84. During the fiscal year 2011 FISMA audit, we documented that disaster recovery tests are not coordinated between OPM's various general support systems. This continues to be an issue, and the existing audit recommendation can be tracked in OIG audit report number 4A-CI-00-11-009.

VIII. Privacy Impact Assessment

FISMA requires agencies to perform a screening 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 any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

The OCIO completed a Privacy Threshold Analysis (PTA) of the LAN/WAN and determined that a PIA was not required for this system because it does not contain personally identifiable information (PII). The assessment concluded that although several applications residing on the LAN/WAN servers contain PII, the OCIO staff supporting the LAN/WAN does not have access to this data.

However, the minor systems that are part of the LAN/WAN have not been subject to a PTA and it is unknown whether any of those systems use or store PII. The OPM Privacy Impact Assessment Guide states that "all OPM IT systems must have a PTA. If the PTA reveals that the system collects no information in identifiable form, for example, the Privacy Program Manager will indicate in the PTA review that no PIA is required. The PTA must be incorporated into the system's certification and accreditation (C&A) package."

Recommendation 5

We recommend that OCIO conduct PTAs for all minor applications residing on the LAN/WAN.

OCIO Response:

"NM – NS concurs with the OIG finding and has created POA&M FY12-Q2-LANWAN-288 and added the POA&M to the Network Management – Network Security POA&M list."

OIG Reply:

As part of the audit resolution process, we recommend that OCIO provide IOC with evidence supporting the remediation of the recommendation.

IX. Plan of Action and Milestones Process

A Plan of Action and Milestones (POA&M) is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The OIG evaluated the LAN/WAN POA&M and verified that it follows the format of OPM's standard template, and has been routinely submitted to the OCIO IT Security and Privacy Group for evaluation. We also determined that the POA&M contained action items for all security weaknesses identified through various security control tests and audits. However, the LAN/WAN POA&M color scheme does not follow the OPM POA&M Standard Operating Procedure (SOP). OPM's POA&M SOP states that POA&Ms are to "use a color scheme where closed items are green, in-progress items are white, items with missed milestones that are delayed less than 90 days are yellow, and items with missed milestones that exceed 90 days are red." There are several instances on the LAN/WAN POA&M where items are classified as ongoing or delayed but are highlighted in green, which indicates that they have been completed. Failure to follow OPM guidelines increases the likelihood that POA&M items are incorrectly identified as complete when the weakness has not been properly remediated.

Recommendation 6

We recommend that OCIO review and update the status of all POA&M items and modify the color scheme to comply with OPM policy.

OCIO Response:

"NM – NS concurs with the OIG finding and has updated the LAN/WAN POA&M list to comply with the OPM color scheme policy. The document is enclosed with this memo."

OIG Reply:

We have reviewed the updated LAN/WAN POA&M and determined that it now accurately follows the color scheme outlined in the OPM POA&M SOP; no further action is required.

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for the LAN/WAN. We tested 48 of the almost 200 security controls outlined in NIST SP 800-53 Revision 3. We tested one or more controls from each of the following control families:

- Access Control
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection
- Program Management

These controls were evaluated by interviewing individuals with LAN/WAN security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 security controls have been successfully implemented for the LAN/WAN, one tested control was not fully satisfied.

a) AC-7 Unsuccessful Login Attempts

The Windows settings related to unsuccessful login attempts do not comply with OPM policy. The Information Security and Privacy Policy Handbook requires that accounts must lock out users after 3 consecutive invalid access attempts and that accounts must be locked out until released by an administrator when the maximum number of invalid attempts is exceeded. [redacted] ailure to abide by OPM Policy and enforce stricter account lockout settings increases the risk that an unauthorized individual could gain access to sensitive OPM resources and data.

Recommendation 7

We recommend that the OCIO modify Windows account lockout settings to comply with OPM policy.

OCIO Response:

"NM – NS concurs with the OIG finding and has created FY12-Q2-LANWAN-295 and added the POA&M to the Network Management – Network Security POA&M list."

OIG Reply:

As part of the audit resolution process, we recommend that OCIO provide IOC with evidence supporting the remediation of the recommendation.

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted] Group Chief
- [redacted], Senior Team Leader
- [redacted], Auditor-in-Charge

Appendix

Memorandum

Office of Personnel Management

March 8, 2012

MEMORANDUM TO: [redacted] Chief, Information Systems Audit Group

FROM: [redacted] Chief, Network Management, Office of the Chief Information Officer

VIA: [redacted], Chief, Information Security Officer, Office of the Chief Information Officer

SUBJECT: FY12 Audit of Local Area Network/Wide Area Network General Support System

The OPM Office of the Inspector General (OIG) has recently completed the draft of their annual FISMA audit of OPM's information technology (IT) systems. The audit of the Office of Personnel Management's (OPM) Local Area Network/Wide Area Network (LAN/WAN) uncovered 7 weaknesses that are listed with the Network Management remediation below.

OIG Finding – Information System Security Plan - Minor System Documentation
The Information System Security Plan (ISSP) contains the majority of the elements outlined by NIST. However, the ISSP does not document minor systems owned and operated by the LAN/WAN.

OIG Recommendation 1
We recommend that the OCIO document all minor applications and the security controls applicable to each on in the LAN/WAN ISSP.

NM Remediation of Recommendation 1
Network Management – Network Security (NM-NS) concurs with the OIG finding and Plan of Action and Milestones (POA&M) item FY12-Q2-LANWAN-287 was created and added to the Network Management – Network Security POA&M list.

- FY12-Q2-LANWAN-287
  Weaknesses: Update the ISSP to include documentation for minor systems/applications
  Milestones with Completion Date: The ISSP will be updated to reflect ownership and security controls testing for any minor systems on the GSS by 8/31/2012 in accordance with the OCIO/ITSP schedule of updates.

OIG Finding – Information System Security Plan - External Interconnections
The ISSP does not contain details of the interconnections between the LAN/WAN and other systems.

OIG Recommendation 2
We recommend that the OCIO revise the LAN/WAN ISSP to include identifiers of the external systems that interconnect with the general support system (name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, name and title of authorizing official).

NM Remediation of Recommendation 2
NM-NS concurs with the OIG finding and Plan of Action and Milestones (POA&M) item FY12-Q2-LANWAN-289 was created and added to the Network Management – Network Security POA&M list.

- FY12-Q2-LANWAN-289
  Weaknesses: Interconnections section does not provide sufficient details concerning external interfaces. OIG recommends OCIO revise the LAN/WAN ISSP to include identifiers of the external systems that interconnect with the general support system (name, organization, type of interconnection, authorizations, dates of agreement, FIPS 199 category, C&A status, name and title of authorizing official).
  Milestones with Completion Dates: Include details about interconnections as part the ISSP update - 8/31/2012.

OIG Finding – Security Control Self-Assessment
The OCIO conducted a self-assessment of the system in August 2011. The assessment included a review of the relevant management, operations, and technical security controls outlined in NIST SP 800-53 Revision 3. However, there is no indication that the security controls of minor applications within the LAN/WAN are tested annually.

OIG Recommendation 3
We recommend that the OCIO test a subset of the security controls for minor systems annually as part of the self-assessment.

NM Remediation of Recommendation 3
NM-NS concurs with the OIG finding and has created POA&M item FY12-Q2-LANWAN-296 and added the item to the Network Management – Network Security POA&M list.

- FY12-Q2-LANWAN-296
  Weaknesses: The OCIO conducted a self-assessment of the system in August 2011. The assessment included a review of the relevant management, operations, and technical security controls outlined in NIST SP 800-53 Revision 3. However, there is no indication that the security controls of minor applications within the LAN/WAN are tested annually.
  Milestones with Completion Dates: Test a subset of the security controls for minor systems as part of the self-assessment by 8/31/12.

OIG Finding – Contingency Plan
The scope of the LAN/WAN contingency plan indicates that it is classified as a high impact system. However, as mentioned above, the security categorization documented in the ISSP identifies the LAN/WAN as a "moderate" system. This inconsistency increases the risk that the scope of security control or contingency plan testing will be inappropriate.

OIG Recommendation 4
We recommend that the OCIO review the contingency plan and the ISSP and address this inconsistency.

NM Remediation of Recommendation 4
NM-NS concurs with the OIG finding and has updated the LAN/WAN Information System Contingency Plan (ISCP). The documented is enclosed with this memo.

OIG Finding – Privacy Impact Assessment
The OCIO completed a Privacy Threshold Analysis (PTA) of the LAN/WAN and determined that a PTA of the LAN/WAN was not required for this system because it does not contain personally identifiable information (PII). The assessment concluded that although several applications residing on the LAN/WAN servers contain PII, the OCIO staff supporting the LAN/WAN does not have access to this data. However, the minor systems that are part of the LAN/WAN have not been subject to a PTA and it is unknown whether any of those systems use or store PII. The OPM Privacy Impact Assessment Guide states that "all OPM IT systems must have a PTA. If the PTA reveals that the system collects no information in identifiable form, for example, the Privacy Program Manager will indicate in the PTA review that no PIA is required. The PTA must be incorporated into the system's certification and accreditation (C&A) package."

OIG Recommendation 5
We recommend that OCIO conduct PTAs for all minor applications residing on the LAN/WAN.

NM Remediation of Recommendation 5
NM – NS concurs with the OIG finding and has created POA&M FY12-Q2-LANWAN-288 and added the POA&M to the Network Management – Network Security POA&M list.

- POA&M FY12-Q2-LANWAN-288
  Weaknesses: Conduct Privacy Threshold Analyses (PTAs) for minor systems/applications.
  Milestones with Completion Dates: PTA's will be conducted on minor applications once they've been identified – 8/31/2012.

OIG Finding – Plan of Action and Milestones Process
The LAN/WAN Plan of Action and Milestones (POA&M) color scheme does not follow the OPM POA&M Standard Operating Procedure (SOP). OPM's POA&M SOP states that the POA&Ms are to "use a color scheme where closed items are green, in-progress items are white, items with missed milestones that are delayed less than 90 days are yellow, and items with missed milestones that exceed 90 days are red." There are several instances on the LAN/WAN POA&M where items are classified as ongoing or delayed but are highlighted in green, which indicates that they have been completed. Failure to follow OPM guidelines increases the chances that POA&M items are incorrectly identified as complete where the weakness has not been properly remediated.

OIG Recommendation 6
We recommend that OCIO review and update the status of all POA&M items and modify the color scheme to comply with OPM policy.

NM Remediation of Recommendation 6
NM – NS concurs with the OIG finding and has updated the LAN/WAN POA&M list to comply with the OPM color scheme policy. The document is enclosed with this memo.

OIG Finding – NIST SP 800-53 Evaluation AC-7, Unsuccessful Login Attempts
The Windows settings related to unsuccessful login attempts do not comply with OPM policy. The Information Security and Privacy Policy Handbook requires that accounts must lock out users after 3 consecutive invalid access attempts and that accounts must be locked out until released by an administrator when the maximum number of invalid attempts is exceeded. The LAN/WAN Group P9olcy Object enforces account lock out after 5 unsuccessful attempts and automatic reset after 15 minutes. Failure to abide by OPM Policy and enforce stricter account lockout settings increase the risk that an authorized individual could gain access to sensitive OPM resources and data.

OIG Recommendation 7
We recommend that the OCIO modify Windows account lockout settings to comply with OPM Policy.

NM Remediation of Recommendation 7
NM – NS concurs with the OIG finding and has created FY12-Q2-LANWAN-295 and added the POA&M to the Network Management – Network Security POA&M list.

- FY12-Q2-LANWAN-295
  Weaknesses: The Windows settings related to unsuccessful login attempts do not comply with OPM policy. The information Security and Privacy Policy Handbook requires that accounts must lock out users after 3 consecutive invalid access attempts and that accounts must be locked out until released by an administrator when the maximum number of invalid attempts is exceeded. [redacted]
  Failure to abide by OPM Policy and enforce stricter account lockout settings increases the risk that an unauthorized individual could gain access to sensitive OPM resources and data.
  Milestones with Completion Dates: Recommend that OCIO modify Windows account lockout settings to comply with OPM Policy.
  - Submit Change Request to address findings by 3/2/12
  - Draft email for agency-wide notice of change by 2/27/12
  - Send agency-wide notice by 3/16/12
  - Implement GPO settings and capture screen shots by 3/23/12
  - Draft WCP, submit with artifacts to ITSP by 3/31/12