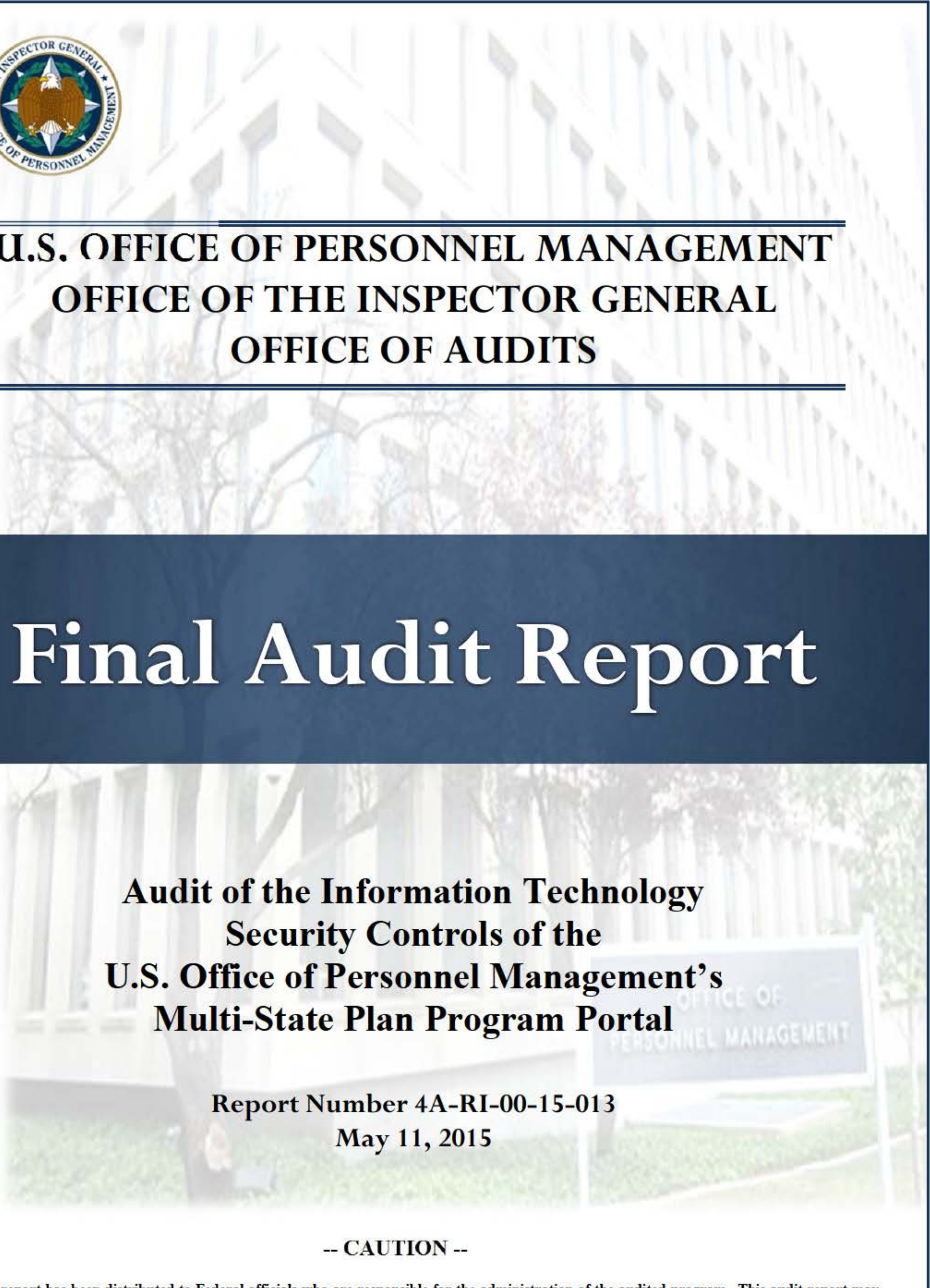

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Multi-State Plan Program Portal

Report Number 4A-RI-00-15-013
May 11, 2015

-- 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 (*http://www.opm.gov/our-inspector-general*), 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.

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Multi-State Plan Program Portal

Report No. 4A-RI-00-15-013 **May 11, 2015**

Why Did We Conduct the Audit?

The Multi-State Plan Program (MSPP) Portal is one of the U.S. Office of Personnel Management's (OPM) critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (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.

What Did We Audit?

The OIG has completed a performance audit of the MSPP Portal to ensure that the system owner, National Healthcare Operations (NHO), has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information Security Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of the IT security controls of the MSPP Portal determined that:

- A Security Assessment and Authorization (SA&A) of the MSPP Portal was completed in October 2014. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.
- The security categorization of the MSPP Portal is consistent with Federal Information Processing Standards (FIPS) 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "Low."
- The MSPP Portal System Security Plan contains the critical elements required by NIST SP 800-18 Revision 1.
- A security control assessment plan and report were completed in June and September 2014, respectively, for the MSPP Portal.
- NHO has performed regular security control self-assessments in accordance with OPM's continuous monitoring methodology.
- A contingency plan was developed for the MSPP Portal that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.
- A privacy threshold analysis was conducted for the MSPP Portal that indicated that a Privacy Impact Assessment (PIA) was not required.
- The MSPP Portal Plan of Acton and Milestones (POA&M) follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool. However, several delayed POA&M items were not updated with new scheduled completion dates in accordance with OPM guidance.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for the MSPP Portal. We determined that a majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4. However, we did note several areas for improvement.

ABBREVIATIONS

FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
GAO	**Government Accountability Office**
HRTT	**Human Resources Tools and Technology**
IG	**Inspector General**
IOC	**Internal Oversight and Compliance**
IT	**Information Technology**
ITSP	**Information Technology Security and Privacy Group**
MSP	**Multi-State Plan**
MSPP	**Multi-State Plan Program**
NHO	**National Healthcare Operations**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIA	**Privacy Impact Analysis**
POA&M	**Plan of Action & Milestones**
PTA	**Privacy Threshold Analysis**
SA&A	**Security Assessment & Authorization**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
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 (FISMA). 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 accordance with FISMA, we audited the information technology (IT) security controls related to the U.S. Office of Personnel Management's (OPM) Multi-State Plan Program (MSPP) Portal.

The MSPP Portal 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.

The MSPP Portal is a web-based application designed to assist National Healthcare Operations (NHO) in receiving, storing and evaluating information received from applicants who wish to become certified Multi-State Plan (MSP) Issuers in the MSPP. The system is currently hosted by AT&T.

We performed preliminary test work of the MSPP Portal in April 2013 when the system was first launched. However, this was our first full scope audit of the security controls surrounding the system. We discussed the results of our audit with NHO representatives at an exit conference. At the end of the fieldwork phase of this audit, NHO informed us that the MSPP Portal will no longer be hosted by AT&T and will be moved to OPM's data center in Macon, Georgia. This move is expected to be completed in May 2015.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

Our objective was to perform an evaluation of the security controls for the MSPP Portal to ensure that NHO officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require owners 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 MSPP Portal, including:

- Security Assessment and Authorization (SA&A);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- System Security Plan (SSP);
- Security Assessment Plan and Report (SAP) and (SAR);
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment (PIA);
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53 Revision 4 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with 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 NHO officials responsible for the MSPP Portal, including IT security controls in place as of January 2015.

We considered the MSPP Portal 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 NHO program office with MSPP Portal security responsibilities, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of the MSPP Portal 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 MSPP Portal of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM’s 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 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;
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

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

The audit was performed by the OPM OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from October 2014 through January 2015 in OPM’s Washington, D.C. office.

Compliance with Laws and Regulations

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

II. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Assessment and Authorization

The Security Assessment and Authorization (SA&A) of the MSPP Portal was completed in October 2013. OPM's Chief Information Security Officer reviewed the MSPP Portal SA&A package and signed the system's authorization letter on October 24, 2013. The system's authorizing official signed the letter and authorized the operational status of the system on October 25, 2013.

NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. The MSPP Portal SA&A appears to have been conducted in compliance with NIST requirements.

B. FIPS 199 Analysis

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 MSPP Portal FIPS Publication 199 Security Categorization analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The MSPP Portal is categorized with a low impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of "low."

The security categorization of the MSPP Portal appears to be consistent with FIPS Publication 199 and NIST SP 800-60 requirements, and we agree with the categorization of "low."

C. System Security Plan

Federal agencies must implement on 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.

The SSP for the MSPP Portal was created using the OCIO’s 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;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the MSPP Portal SSP and determined that it adequately addresses each of the elements required by NIST. Nothing came to our attention to indicate that the system security plan of the MSPP Portal has not been properly documented and approved.

D. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for the MSPP Portal in June 2013 and September 2013, respectively, as a part of the system’s SA&A process. The SAP and SAR were completed by a contractor that was operating independently from NHO. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a “low” security categorization according to NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems.

The SAR identified four control weaknesses; these weaknesses were appropriately added to the MSPP Portal POA&M. All weaknesses identified were classified with a low risk rating.

Nothing came to our attention to indicate that the security controls of the MSPP Portal have not been adequately tested by an independent source, or that weaknesses identified have not been properly documented.

E. Continuous Monitoring

OPM's Information Security and Privacy Policy Handbook states that continuous monitoring security reports must be provided to the OCIO's Information Technology Security and Privacy Group (ITSP) at least semiannually. The OCIO also creates continuous monitoring plans each fiscal year that clearly describe the type and frequency of NIST SP 800-53 Revision 4 security controls that must be tested throughout the year.

In FY 2014, NHO submitted adequate evidence of continuous monitoring security control testing for the MSPP Portal to the ITSP in a timely manner.

Nothing came to our attention to indicate NHO's continuous monitoring activities were not in compliance with OPM guidelines.

F. 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 disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The MSPP Portal contingency plan documents the functions, operations, and resources necessary to restore and resume the MSPP Portal operations when unexpected events or disasters occur. The MSPP Portal contingency plan follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A contingency plan test of the MSPP Portal was conducted in August 2014. The test involved a discussion-based exercise of recovering the system at the backup data center and then returning operations to the regular data center. The testing documentation contained adequate analysis and review of the test results.

G. Privacy Impact Assessment

FISMA requires agencies to perform a screening of federal information systems to determine if a 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.

NHO completed an initial privacy screening or Privacy Threshold Analysis (PTA) of the MSPP and determined that a PIA was not required for this system. The PTA for the MSPP Portal appears consistent with FISMA and OPM requirements, and we agree a PTA was sufficient and a PIA is not required.

H. Plan of Action and Milestones Process

A 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.

We evaluated the MSPP Portal POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for evaluation. We determined that the weaknesses discovered during the SA&A security assessment were included in the POA&M.

However, we noted four items on the POA&M that were over 180 days overdue with a status of "delayed" that did not indicate a new scheduled completion date. OPM POA&M Standard Operating Procedures state that "If the weakness is not addressed by the scheduled completion date, the new scheduled completion date must be addressed in the Milestone Changes column, along with the updated milestones and dates necessary to achieve the new scheduled completion date."

Failure to update a system's POA&M with material changes increases the likelihood of weaknesses not being addressed in a timely manner and therefore exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 1

We recommend that NHO update the MSPP Portal POA&M with new scheduled completion dates for all delayed items.

HI Response:

"The POA&M has been updated for all delayed items. The estimated completion date for MA-4 is now 2015-06-30. All other weaknesses have been completed. Staff in OPM's Chief Information Officer/IT Security Policy office updated Trusted Agent (see attached)."

OIG Reply:

Evidence was provided in response to the draft audit report to indicate that new scheduled completed dates have been updated for delayed items or have been remediated since the issuance of the draft report; no further action is required.

I. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for the MSPP Portal. We tested approximately 50 security controls outlined in NIST SP 800-53 Revision 4 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. 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
- Identity and Authentication
- Incident Response
- Maintenance
- Media Protection
- Planning
- Risk Assessment
- System and Communications Protection
- System and Information Integrity

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

We determined that the tested security controls appear to be in compliance with NIST SP 800-53 Revision 4 requirements with a few exceptions. The following recommendations are directed at the current version of the system hosted by AT&T. However if these issues are not remediated before the system is moved to OPM's internal data center, the recommendations should still be implemented on the new platform, as moving to the new platform does not inherently resolve these issues.

1. **RA-5 Vulnerability Scanning**

We independently performed automated vulnerability scans on a sample of servers, databases and web applications. The detailed results of the scans were provided to NHO, but for security purposes will not be described in this report. A high level summary of the results is below.

System Patching

The vulnerability scans performed during the audit indicate that critical patches and service packs are not always implemented in a timely manner for the operating platforms supporting the MSPP Portal.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 states that the organization must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly.

Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 2

We recommend that NHO implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.

HI Response:

"We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015 rather than May 2015. OPM's Chief Information Officer/Operations Technology Management has the lead now for installing patches, service packs, hotfixes, as well as conducting vulnerability scans, on a timely basis."

OIG Reply:

The response to the draft report indicated that the MSPP has migrated to OPM's Macon, Georgia hosting environment and is now managed by OPM's OCIO. However, the transition alone is not sufficient evidence to close the recommendation. The intent of the recommendation was for the program office to establish a control methodology to ensure servers and databases are routinely updated with patches, service packs, and hotfixes. As part of the audit resolution process, we recommend that NHO provide OPM's Internal Oversight and Compliance (IOC) division with additional evidence to support that a methodology has been implemented to ensure that servers and databases are updated in a timely manner.

Noncurrent Software

The results of the vulnerability scans indicated that several servers supporting the MSPP Portal contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

<u>Recommendation 3</u>

We recommend that NHO implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

<u>HI Response:</u>

"We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015. OPM's Web Team verified that no outdated system software migrated with the MSP Application Portal to Macon, Georgia, and verified that there is no outdated software saved on the Macon, Georgia production server that hosts the MSP Application Portal."

<u>OIG Reply:</u>

The response to the draft report indicated that OPM's Web Team verified that no outdated system software was migrated along with the application portal to the OPM Macon, Georgia hosting environment. However, the intention of this recommendation was for the program office to establish a routine audit process to ensure that only current, supported versions of the system software are installed on production servers going forward. As part of the audit resolution process, we recommend that NHO provide OPM's IOC division with evidence that controls that address this issue are in place in the system's new environment.

Insecure Configurations

The results of the vulnerability scans also indicated that the web application for the MSPP Portal is insecurely configured in a manner that is susceptible to several malicious attack methods.

These malicious activities include, but are not limited to:

- [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Failure to remediate these vulnerabilities increases the risk of not only the web application and backend data to hackers, but the organization as a whole, as a breach in a single access point could lead to the whole network environment being exposed.

Recommendation 4

We recommend that NHO **immediately** remediate vulnerabilities discovered as a result of the vulnerability scans conducted during this audit.

HI Response:

"We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015. OPM's Chief Information Officer/Operations Technology Management has the lead now for conducting vulnerability scans on a regular basis.

Since the MSP Application Portal is now hosted in Macon, Georgia, we would welcome the OIG to perform a vulnerability scan and we would commit to resolving any vulnerabilities detected."

OIG Reply:

Moving the application from one data center to another does not have an impact on the web application code or the vulnerabilities we identified; the original recommendation remains applicable.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Healthcare and
Insurance

March 10, 2015

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

FROM: [redacted]
Deputy Assistant Director
Healthcare and Insurance
National Healthcare Operations

SUBJECT: Reply to Draft Audit Report No. 4A-RI-00-15-013

Thank you for providing us the opportunity to respond to the U.S. Office of Personnel Management's Office of the Inspector General (OIG) draft report, *Audit of the Information Technology Security Controls of the OPM's Multi-State Plan Program Portal* (Report No. 4A-RI-00-15-013).

We recognize that even the most well run programs benefit from external evaluations, and we appreciate your input as we continue to enhance our programs. Responses to your recommendations are provided below.

Recommendation 1: We recommend NHO update the MSPP Portal POA&M with new scheduled completion dates for all delayed items.

Management Response: We concur. The POA&M has been updated for all delayed items. The estimated completion date for MA-4 is now 2015-06-30. All other weaknesses have been completed. Staff in OPM's Chief Information Officer/IT Security Policy office updated Trusted Agent (see attached).

Recommendation 2: We recommend that NHO implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.

Management Response: We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015 rather than May 2015. OPM's Chief Information Officer/Operations Technology Management has the lead now for installing patches, service packs, hotfixes, as well as conducting vulnerability scans, on a timely basis.

Recommendation 3
We recommend that NHO implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

Management Response: We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015. OPM's Web Team verified that no outdated system software migrated with the MSP Application Portal to Macon, Georgia, and verified that there is no outdated software saved on the Macon, Georgia production server that hosts the MSP Application Portal.

Recommendation 4
We recommend that NHO **immediately** remediate vulnerabilities discovered as a result of the vulnerability scans conducted during this audit.

Management Response: We concur. The MSP Application Portal migrated from AT&T's hosting environment in Ashburn, Virginia to OPM's Macon, Georgia hosting environment on February 25, 2015. OPM's Chief Information Officer/Operations Technology Management has the lead now for conducting vulnerability scans on a regular basis.

Since the MSP Application Portal is now hosted in Macon, Georgia, we would welcome the OIG to perform a vulnerability scan and we would commit to resolving any vulnerabilities detected.

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

cc: [redacted], CIO/Information Technology System Policy
, CIO/Information Technology System Policy
, MSAC/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