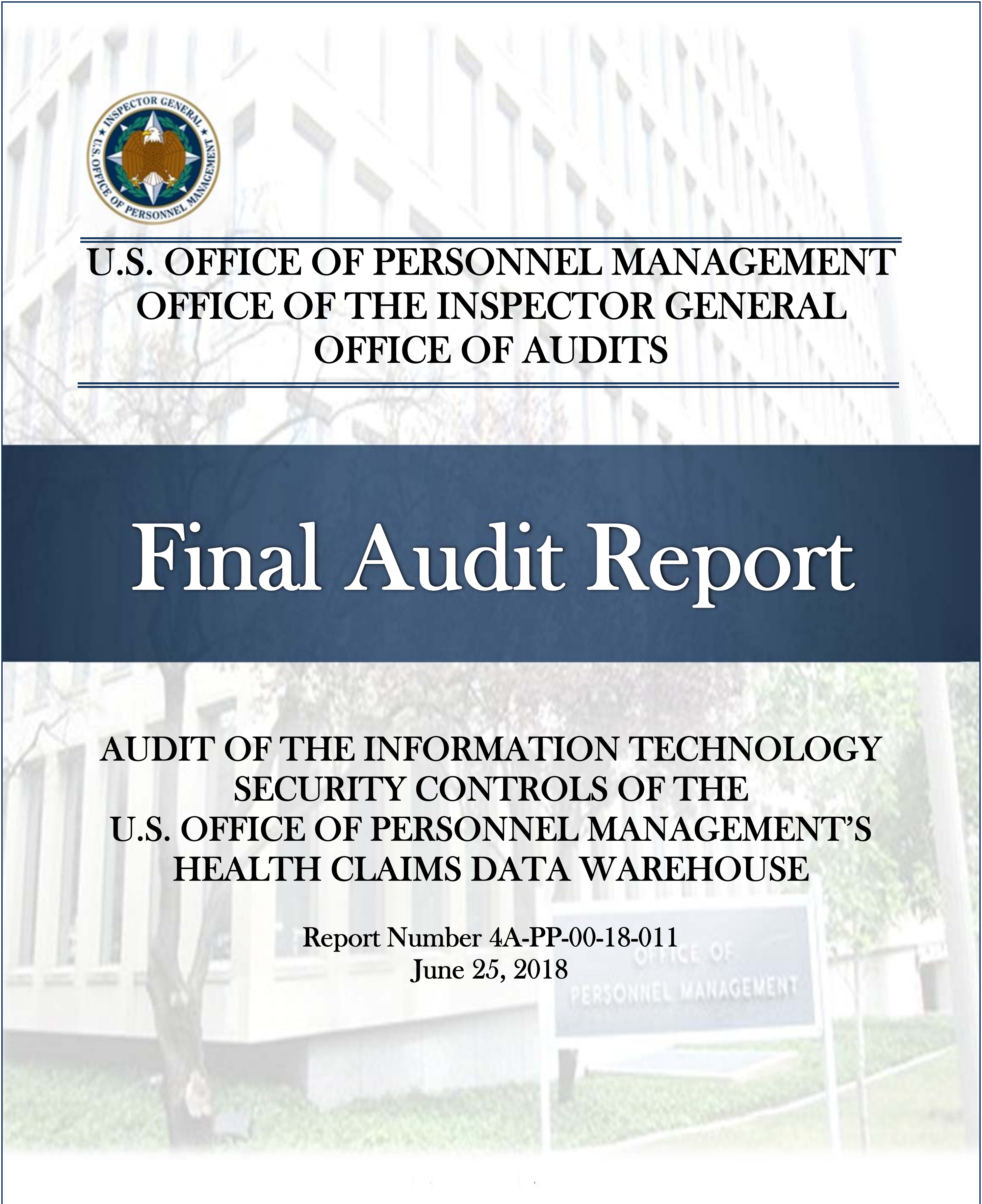

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S HEALTH CLAIMS DATA WAREHOUSE

Report Number 4A-PP-00-18-011
June 25, 2018

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the
U.S. Office of Personnel Management's
Health Claims Data Warehouse

Report No. 4A-PP-00-18-011 **June 25, 2018**

Why Did We Conduct the Audit?

The Health Claims Data Warehouse (HCDW) is one of the U.S. Office of Personnel Management's (OPM) major information technology (IT) systems. The Federal Information Security Modernization Act requires that the Office of the Inspector General perform an audit of IT security controls of this system.

What Did We Audit?

The Office of the Inspector General completed a performance audit of the HCDW to ensure that the system's security controls meet the standards established by the Federal Information Security Modernization Act, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, 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 HCDW determined that:

- The HCDW Security Assessment and Authorization was in place through May 2018. At the time of this audit, work on a new Authorization was underway and a one year Authorization granted through May 2019.
- The HCDW security categorization is consistent with both the Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60, and we agree with the "high" categorization.
- OPM completed a Privacy Impact Assessment for the HCDW.
- The HCDW System Security Plan follows the OCIO template, but did not adequately reflect the current state of the system.
- A full security controls assessment was completed for the HCDW in January 2015, however many of the assessed controls were incorrectly labeled in relation to the system's "high" categorization.
- The HCDW has not been subject to routine continuous monitoring testing.
- OPM developed and tested a contingency plan for the HCDW, however the plan has not been updated to account for major changes to the system.
- The HCDW Plan of Action and Milestones documentation does not contain all OPM required fields and several of the weaknesses have not been remediated timely.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined most of the security controls tested appear to be in compliance, however we did note several areas for improvement.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Modernization Act**
HCDW	**Health Claims Data Warehouse**
IT	**Information Technology**
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**
PDS	**Program Development and Support**
POA&M	**Plan of Action and Milestones**
SP	**Special Publication**

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 evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of Inspector General 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.

The Health Claims Data Warehouse (HCDW) is one of the agency's major information technology systems. The U.S. Office of Personnel Management (OPM) uses the HCDW to receive, store, and analyze health insurance claims from fee-for-service insurance carriers. The Health and Insurance, Program Development and Support (PDS) office also uses the HCDW to review data from health maintenance organizations to support management and administrative purposes for the Federal Employees Health Benefits Program. This was our first audit of the HCDW information technology controls.

OPM's Office of the Chief Information Officer (OCIO) and the PDS office share responsibility for implementing and managing the information technology (IT) security controls of the HCDW. We discussed the results of our audit with the OCIO and PDS representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an audit of the security controls for the HCDW to ensure that OCIO and PDS officials 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, and OPM's OCIO.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements were implemented for the HDCW, including:

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- Privacy Impact Assessment;
- System Security Plan;
- Security Assessment Plan and Report;
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

SCOPE AND METHODOLOGY

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

FISMA compliance efforts of OPM officials responsible for the HCDW, including the evaluation of IT security controls in place as of January 2018.

We considered the HCDW 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 and PDS office with security responsibilities for the HCDW, 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 HCDW are located in the "Audit Findings and Recommendations" 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 HCDW internal controls taken as a whole. The criteria used in conducting this audit include:

- OPM Information Security Privacy and Policy Handbook;

- OMB Circular A-130, Appendix I, Responsibilities for Protecting and Managing Federal Information Resources;

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

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

- The Federal Information System Controls Audit Manual;

- NIST SP 800-12, Revision 1, An Introduction to Information 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 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, we conducted the audit in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The OPM Office of the Inspector General performed the audit, as established by the Inspector General Act of 1978, as amended. The OIG conducted the audit from November 2017 through January 2018 at OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's management of the HCDW is consistent with applicable standards. While generally compliant, with respect to the items tested, OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY ASSESSMENT AND AUTHORIZATION

The HCDW was authorized to operate until May 9, 2019.

A Security Assessment and Authorization (Authorization) includes 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement.

However, OPM does not yet have a mature program in place to continuously monitor system security controls, therefore an Authorization is required for all OPM systems at least once every three years as required by OPM policy.

In November 2015 OPM granted an initial Authorization to Operate to the HCDW that expired after one year. Based on a review of the system documentation, controls, and POA&M efforts, the OCIO granted the HCDW a continuation of the Authorization to Operate until May 11, 2018.

At the time of the audit, OPM was actively working to complete an Authorization and receive a new Authorization to Operate for HCDW. A one year Authorization to Operate was granted through May 9, 2019. This effort was not included in the scope of this audit.

Nothing came to our attention to indicate that the HCDW Authorization to Operate was inadequate.

B. FIPS 199 ANALYSIS

The E-Government Act of 2002 requires Federal agencies to categorize all Federal information and information systems. FIPS 199 provides guidance on how to assign appropriate categorization levels for information security according to a range of risk levels.

NIST SP 800-60 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 HCDW security categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The HCDW has a "high" confidentiality and integrity impact, resulting in an overall system categorization of "high."

Nothing came to our attention to indicate that the HCDW security categorization was inadequate.

C. **PRIVACY IMPACT ASSESSMENT**

The E-Government Act of 2002 requires agencies to perform a Privacy Threshold Analysis of Federal information systems to determine if a Privacy Impact Assessment is required for that system. A Privacy Threshold Analysis was performed on the HCDW in February 2015, and it was determined that a Privacy Impact Assessment was required for this system.

OMB Memorandum M-03-22 outlines the necessary components of a Privacy Impact Assessment. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system. The Privacy Impact Assessment was complete and was formally approved and signed by the Chief Privacy Officer in April 2015.

We did not detect any issues with the Privacy Impact Assessment performed for the HCDW.

D. **SYSTEM SECURITY PLAN**

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

The PDS office developed the HCDW SSP using the OCIO's SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. The template requires the SSP to contain the following elements:

- System Name and Identifier;
- Authorizing Official;
- Assignment of Security Responsibility;
- System Owner;
- Other Designated Contacts;
- System Operational Status;

- General Description/Purpose;
- Information System Type;
- System Environment;
- System Interconnection/Information Sharing;
- System Categorization;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the current HCDW SSP, signed in November 2015, and determined that it does not adequately reflect the system's current state. The most apparent flaw is that the SSP identifies the system as in development, while in reality, the HCDW has been in production since October 2016. Moving a system from development to production is a significant change in system status and functionality that should require re-evaluation and Authorization.

NIST SP 800-18, Revision 1, states "it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system."

The lack of a current and accurate SSP increases the risks that controls are not implemented and functioning as required. This also increases the difficulty of assessing and addressing risks to the system and to OPM as a whole.

Recommendation 1

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

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and agrees to work with the OPM Cybersecurity Program to update SSP based on the recommendation."

OIG Comment:

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

E. SECURITY ASSESSMENT PLAN AND REPORT

OPM completed the HCDW Security Assessment Plan in December 2014 and the HCDW Security Assessment Report in January 2015. Both the assessment and documentation were completed while the system was in the development phase, prior to the initial authorization and move to production. OPM also conducted a risk assessment in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments.

We verified that appropriate management, operational, and technical controls were tested for a system with a "high" security categorization. However, we observed that 52 inherited controls of the 343 controls tested were incorrectly labeled as "Not Applicable." The assessors did not clarify why these controls were considered "Not Applicable" to the HCDW assessment. This demonstrates the strong possibility that additional controls may have been identified incorrectly and more weaknesses exist than the assessment identified.

According to OPM policy, "Security controls assessment[s] shall be conducted . . . to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."

We are aware that OPM plans to update the Security Assessment Plan and conduct a new assessment as part of the 2018 Authorization. However, failure to completely assess the controls and ensure they are meeting the system security requirements can leave the system vulnerable. Unidentified and undocumented weaknesses increase the potential for exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 2

We recommend that OPM ensure a full independent security controls assessment of the HCDW is conducted based on an updated Security Assessment Plan.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made and agrees to address the recommendation. As OIG noted in the report, management plans to execute a full independent security assessment of HCDW based on the updated SSP in 2018."

F. CONTINUOUS MONITORING

The HCDW security controls were not subject to routine testing as a part of continuous monitoring.

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous Monitoring Plan template to each individual system's specific security control needs and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

As a part of our general FISMA audit for FY 2017, we did not receive adequate evidence of the HCDW quarterly continuous monitoring submissions to the OCIO.

Currently, there is an open recommendation in the FY 2017 FISMA audit report (Report No. 4A-CI-00-17-20, Recommendation 35) that requires all OPM systems to complete an annual test of controls and we continue to recommend that the HCDW adhere to the OCIO's established guidelines.

G. CONTINGENCY PLANNING AND CONTINGENCY PLAN TESTING

NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

1) Contingency Plan

OPM completed the HCDW contingency plan in November 2015 while the system was in development. Despite transitioning to a production environment and a contingency plan test in 2017, OPM has not reviewed or updated the plan. The plan also contains out of date and/or inaccurate information for how the system receives data, the contingency planning team responsibilities, and the system diagrams. In addition, we could not confirm the existence of supporting documentation including: recovery procedures, validation plans, and backup procedures.

According to OPM policy, "[The system owner] shall ensure . . . the contingency plan is reviewed for the information system at least annually . . . [and is revised] to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing . . . ."

An outdated and inaccurate contingency plan can cause additional confusion and prolonged outages during an incident.

Recommendation 3

We recommend that OPM update the HCDW contingency plan in accordance with the OPM template and policies.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will coordinate with the OPM Cybersecurity Program to update the HCDW contingency plan in accordance with the OPM template and policies."

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans for all systems be tested annually to evaluate the plan's effectiveness and the organization's readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

OPM conducted the most recent HCDW contingency plan test in October 2017. Documentation from the test showed valid results to a functional test exercise, updated contact information for the exercise planning team, and a thorough improvement plan.

Nothing came to our attention to indicate that the HCDW contingency plan testing process was inadequate.

H. PLAN OF ACTION AND MILESTONES

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

1) Incomplete and Outdated POA&Ms

The HCDW POA&M does not adhere to the required OPM template.

The HCDW POA&M does not adhere to the required OPM template. As a result, the POA&M is missing required and critical information about identified weaknesses including estimated and actual completion dates, resources required, and any milestone changes.

The HCDW POA&M lists 22 security weaknesses dating back to FY 2015. Of these 22 outstanding weaknesses, none have updated remediation plans or timelines. If remediation is delayed or the original due date deemed unrealistic, it is imperative the POA&M documentation be updated so that the current risks to the system can be understood and resources most efficiently used to address risk.

OPM's guidance "mandates that the POA&M template . . . be populated and updated for the quarterly and annual submission." Furthermore, OPM's guidance states that "Should expected completion dates for milestones of POA&Ms be missed, the associated POA&Ms will be brought before the [Management Review Board] for review in order to address any corrective actions needed for remediating the POA&Ms in accordance with the requirements defined in the Authorization to Operate . . . issued for the applicable system. Updated milestones and expected completion dates will be required for the following [Management Review Board] meeting."

Failure to utilize the required template can lead to the omission of critical information and inhibit the remediation of known security weaknesses. Failure to update a POA&M increases the likelihood of weaknesses not being addressed in a timely manner and potentially exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

<u>Recommendation 4</u>

We recommend that OPM update the HCDW POA&M to include all required information and follow the requirements outlined in OPM's POA&M policy and template.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to coordinate with the OPM Cybersecurity Program in updating all HCDW POA&Ms, to include all required information as outlined in OPM's POA&M policy and template."

Recommendation 5

We recommend that OPM develop a detailed action plan to remediate all of the overdue HCDW POA&M items. This action plan should include realistic estimated completion dates and milestones and be presented to the Management Review Board.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to coordinate with the OPM Cybersecurity Program to develop a plan with estimated completion dates and milestones to address HCDW POA&M deficiencies. Management will present the POA&M action plan to the Management Review Board for review."

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 OPM has implemented a subset of these controls for the HCDW. We tested approximately 40 controls as outlined in NIST SP 800-53, Revision 4, including one or more controls from each of the following control families:

- Access Control;
- Awareness and Training;
- Contingency Planning;
- Incident Response;
- Planning;
- Audit and Accountability;
- Configuration Management;
- Identity and Authentication;
- Media Protection;
- Risk Assessment;

- Security Assessment and Authorization;
- System and Information Integrity; and
- System and Communications Protection;
- System and Services Acquisition.

These controls were evaluated by interviewing individuals with system security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system. We determined that the majority of the tested security controls appear to be in compliance with NIST SP 800-53, Revision 4, requirements with the exceptions detailed below.

1) Control AC-6 – Least Privilege

During the course of our audit, we observed a number of nonessential users with privileged access to a majority of the HCDW servers. OPM has acknowledged the unnecessary group of users and plans to remove their access to the servers.

According to OPM policy, "[System owners] shall ensure the concept of least privilege is employed, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Not enforcing the principle of least privilege can subject a system to unauthorized access and further jeopardize the system's security.

Recommendation 6

We recommend that OPM review all HCDW user access and remove unnecessary privileged access to the HCDW servers.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and agrees to address the recommendation. All unnecessary privileged access will be removed from HCDW servers and access controls will be reviewed on a routine basis."

2) Control AC-17 – Remote Access

System documentation indicates that remote access connections to the HCDW are not allowed. However, OPM has not implemented technical controls to ensure users are restricted from accessing the system remotely.

OPM has not implemented technical controls to ensure users are restricted from accessing the system remotely.

NIST SP 800-53, Revision 4, requires that the organization "Establishes and documents usage restrictions [and] configuration/connection requirements . . . ." The guidance also requires that "The information system monitors and controls remote access methods."

Failure to implement controls restricting remote access to the HCDW increases the risk that the system is subject to brute force and malicious attacks from external sources. This also means that HCDW users currently have the ability to improperly access the system outside of their approved work environment.

Recommendation 7

We recommend that OPM implement technical controls to ensure that remote access is restricted for the HCDW.

OPM Response:

"Partially concur - Management agrees with the underlying finding that led to the recommendation. However, the original system documentation was written at a time when remote access to HCDW was not permitted. Management will update the security documentation to reflect the current security controls allowing remote access."

OIG Comment:

Before changing the security controls documentation, we recommend that the PDS office conduct a risk assessment for allowing remote access and formally accept any risk identified. As part of the audit resolution process, we recommend that the PDS office provide OPM's Internal Oversight and Compliance office with evidence of the risk assessment for allowing remote access to the HCDW, and the risk acceptance, along with the updated system documentation reflecting the policy and procedure changes.

3) Control AT-4 – Security Training Records

OPM documents the completion of OPM's annual security awareness training for all HCDW users. However, OPM does not document, monitor, or maintain specialized training specific to HCDW users and account managers.

NIST SP 800-53, Revision 4, requires that an organization "Documents and monitors information system security training activities including basic security awareness training and specific system security training . . . ."

The lack of documentation and monitoring of specialized training for HCDW users and account managers increases the likelihood of inadequate user training and therefore more potential user errors and system vulnerabilities.

Recommendation 8

We recommend that OPM document specialized training requirements and ensure HCDW users and account managers complete those requirements.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made and will document the completion of specialized training in accordance with OPM Cybersecurity Policy."

4) Control CA-8 – Penetration Testing

OPM acknowledged that a current penetration test was not conducted for the HCDW, despite the most recent assessment identifying this control as Fully Satisfied. OPM plans to conduct a full penetration test on the system during the next authorization cycle in May 2018.

NIST SP 800-53, Revision 4, requires that "The organization conducts penetration testing" for high rated systems like the HCDW.

Not performing a penetration test increases the likelihood of vulnerabilities remaining undetected and that a vulnerability is exploited.

Recommendation 9

We recommend that OPM conduct a penetration test on the HCDW.

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to conduct penetration testing in accordance with OPM Cybersecurity Program policy."

5) [redacted]

[redacted]

[redacted]

[redacted]

Recommendation 10

We recommend that OPM implement [redacted].

OPM Response:

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will coordinate with the OPM Cybersecurity Program to [redacted]"

6) Control CM-6 – Configuration Settings

Approved configuration settings are documented for some but not all of the operating platforms used by the HCDW. While the configuration settings provided were adequate, OPM still needs to formally document and approve the configuration settings for the remaining operating platforms.

NIST SP 800-53, Revision 4, requires that an organization "Establishes and documents configuration settings for information technology products employed within the information system . . . ."

Approved configuration settings are not documented for all of the operating platforms used by the HCDW.

Failure to document standard configuration settings for all information systems increases the risk of an insecurely configured system being more susceptible to attack.

OPM is aware of this issue and has an open POA&M from FY 2015 (FY15-Q3-HCDW-01) to document these standard configuration settings. Despite OPM developing adequate configuration settings for some of the HCDW operating platforms, addressing the remainder of the operating platform configurations is necessary to remediate the outstanding POA&M weakness.

Additionally, there is an open recommendation in the FY 2017 FISMA audit report (Report No. 4A-CI-00-17-20, Recommendation 20) that requires OPM to develop and implement standard configuration settings for all operating platforms in use by OPM.

7) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

<u>Recommendation 11</u>

We recommend that OPM [redacted]

<u>OPM Response:</u>

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will [redacted]

8) Control RA-5 – Vulnerability Scanning

During our audit, it came to our attention that one of the HCDW servers was not included in the OPM scanning inventory. OPM has acknowledged that the server was not included in the scanning inventory.

OPM policy states that the "System Owners . . . shall ensure . . . Scanning for vulnerabilities in the information system and hosted applications is completed at least quarterly for high systems and semi-annually for other systems, and when new vulnerabilities potentially affecting the system/applications are identified and reported."

Failure to scan system servers can leave the system vulnerable to security breaches.

<u>Recommendation 12</u>

We recommend that OPM ensure all HCDW servers are included in the vulnerability scanning inventory and that routine vulnerability scans are conducted on these servers.

<u>OPM Response:</u>

"Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will include all HCDW servers in routine vulnerability scans."

APPENDIX

April 20, 2018

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

FROM: DAVID A. GARCIA
CHIEF INFORMATION OFFICER

ALAN P. SPIELMAN
DIRECTOR, HEALTHCARE AND INSURANCE

Subject: Office of Personnel Management Response to the Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Health Claims Data Warehouse (Report No. 4A-PP-00-18-011)

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Health Claims Data Warehouse, Report Number 4A-PP-00-18-011. The OIG comments are valuable to the Agency 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, our private industry partners, and the public.

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

Recommendation #1: We recommend that OPM update the HCDW SSP to reflect the current state of the system and ensure it meets OPM policies and NIST guidelines.

Concur – Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and agrees to work with the OPM Cybersecurity Program to update SSP based on the recommendation.

Recommendation #2: We recommend OPM ensure a full independent security controls assessment of the HCDW is conducted based on an updated Security Assessment Plan.

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made and agrees to address the recommendation. As OIG noted in the report, management plans to execute a full independent security assessment of HCDW based on the updated SSP in 2018.

Recommendation #3: We recommend OPM update the HCDW contingency plan in accordance with the OPM template and policies.

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will coordinate with the OPM Cybersecurity Program to update the HCDW contingency plan in accordance with the OPM template and policies.

Recommendation #4: We recommend that OPM update the HCDW POA&M to include all required information and follow the requirements outlined in OPM's POA&M policy and template.

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to coordinate with the OPM Cybersecurity Program in updating all HCDW POA&Ms, to include all required information as outlined in OPM's POA&M policy and template.

Recommendation #5: We recommend that OPM develop a detailed action plan to remediate all the overdue HCDW POA&M items. This action plan should include realistic estimated completion dates and milestones and be presented to the Management Review Board.

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to coordinate with the OPM Cybersecurity Program to develop a plan with estimated completion dates and milestones to address HCDW POA&M deficiencies. Management will present the POA&M action plan to the Management Review Board for review.

Recommendation #6**:** We recommend OPM review all HCDW user access and remove unnecessary privileged access to the HCDW servers.

Concur – Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and agrees to address the recommendation. All unnecessary privileged access will be removed from HCDW servers and access controls will be reviewed on a routine basis.

Recommendation #7: We recommend OPM implement technical controls to ensure that remote access is restricted for the HCDW.

Partially concur – Management agrees with the underlying finding that led to the recommendation. However, the original system documentation was written at a time when remote access to HCDW was not permitted. Management will update the security documentation to reflect the current security controls allowing remote access.

Recommendation #8: We recommend that OPM document specialized training requirements and ensure HCDW users and account managers complete those requirements.

Concur – Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made and will document the completion of specialized training in accordance with OPM Cybersecurity Policy.

Recommendation #9: We recommend that OPM conduct a penetration test on the HCDW.

Concur – Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and plans to conduct penetration testing in accordance with OPM Cybersecurity Program policy.

Recommendation #10: We recommend OPM implement [redacted].

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will coordinate with the OPM Cybersecurity Program to [redacted]

Recommendation #11: We recommend that OPM [redacted].

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and [redacted]

Recommendation #12: We recommend OPM ensure all HCDW servers are included in the vulnerability scanning inventory and that routine vulnerability scans are conducted on these servers.

Concur - Management agrees with the underlying findings that led to the recommendation, acknowledges that improvements could be made, and will include all HCDW servers in routine vulnerability scans.

In addition to providing these responses to your recommendations, we also conducted a sensitivity review of the information contained in your report to determine if there were any aspects that should be shielded from public disclosure. We identified two recommendations that contained information that we would not publicly release. First, Recommendation 10 includes specific details about the HCDW processes for handling sensitive data. In addition, Recommendation 11 provides specific details about access control implementation for users accessing HCDW.

We are concerned that this information, if made public, could provide insights to potential adversaries regarding access controls and how the system handles sensitive data. This disclosure would leave us vulnerable to the risk of cyber attack that could be avoided if the information is redacted or changed. Upon request, we can provide you with the specific statements that we would propose for redaction or suggest some alternative language that we would be comfortable with releasing.

We appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mr. Jeffrey Wagner or [redacted].

cc:
Robert M. Leahy
Deputy Chief Information Officer

Jeffrey P. Wagner
Associate Chief Information Officer for Enterprise Infrastructure Solutions

Janet L. Barnes
Director, Internal Oversight and Compliance

Michael D. Dovilla
Chief of Staff

Theodore M. Cooperstein
General Counsel

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