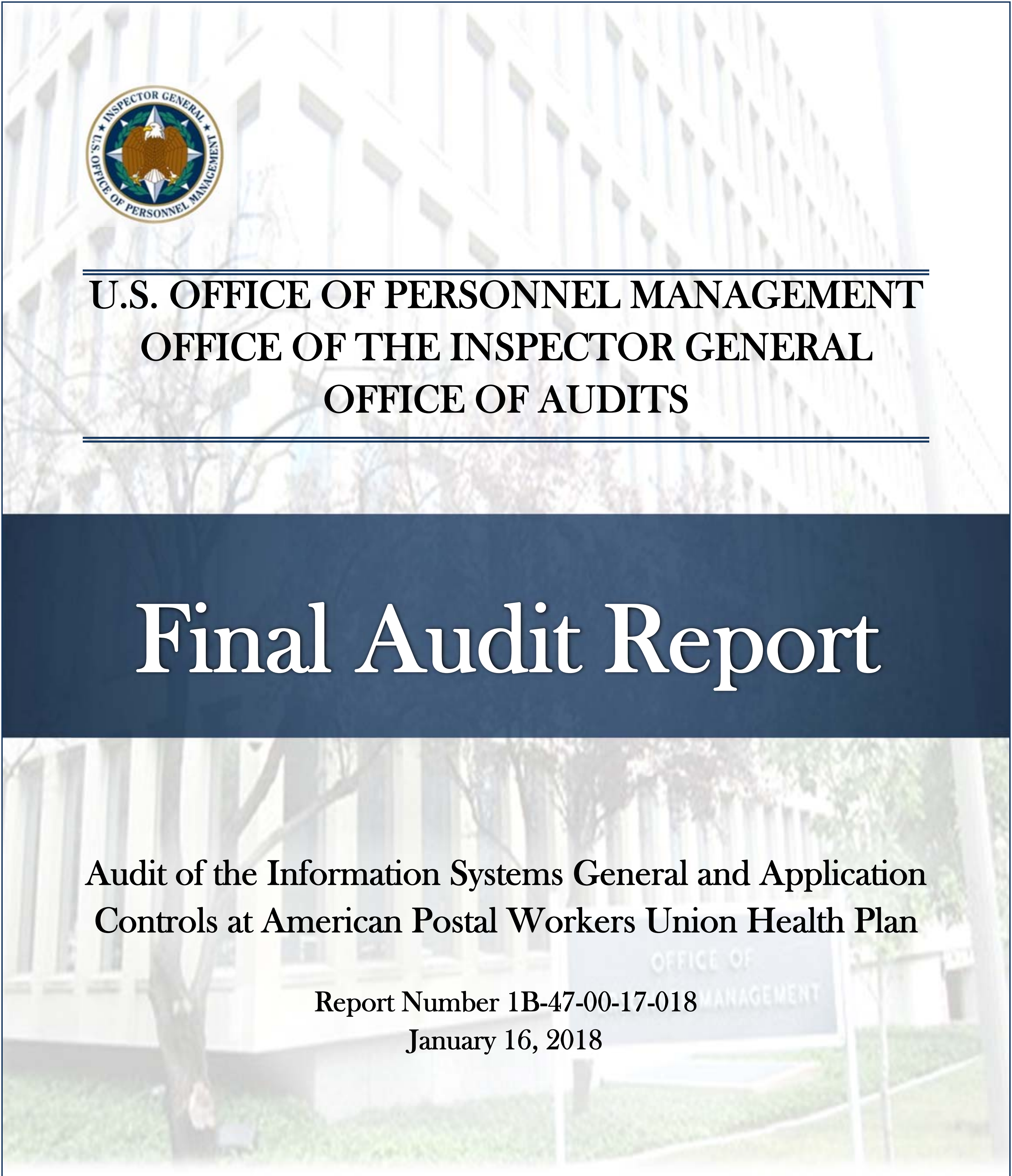

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

# Final Audit Report

## Audit of the Information Systems General and Application Controls at American Postal Workers Union Health Plan

Report Number 1B-47-00-17-018
January 16, 2018

# EXECUTIVE SUMMARY

*Audit of the Information Systems General and Application Controls at American Postal Workers Union Health Plan*

**Report No. 1B-47-00-17-018** **January 16, 2018**

## Why Did We Conduct the Audit?

American Postal Workers Union Health Plan (APWUHP) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in APWUHP's information technology (IT) environment.

## What Did We Audit?

The scope of this audit centered on the information systems used by APWUHP to process and store data related to insurance claims for FEHBP members.

**Michael R. Esser**
***Assistant Inspector General for Audits***

## What Did We Find?

Our audit of the IT security controls of APWUHP determined that:

- APWUHP has established an adequate security management program. However, there is not a policy requiring role-based training for IT security staff.
- APWUHP has implemented a variety of physical and logical access controls. However, we noted several areas of concern related to data center physical access controls, physical and logical access reviews, and privileged user access.
- APWUHP has implemented an incident response and network security program. However, we noted several areas of concern related to firewall management, network access controls, and incident response testing.
- APWUHP has developed formal configuration management policies and procedures. However, APWUHP does not have documented security configuration standards, and does not routinely review systems for configuration compliance.
- APWUHP has developed and documented a formal business continuity and disaster recovery plan that contains the elements suggested by relevant guidance and publications.
- APWUHP has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, physical claims storage should be improved.

# ABBREVIATIONS

| | |
|---|---|
| **APWUHP** | **American Postal Workers Union Health Plan** |
| **CFR** | **Code of Federal Regulations** |
| **FEHBP** | **Federal Employees Health Benefits Program** |
| **FISCAM** | **Federal Information Security Controls Audit Manual** |
| **GAO** | **U.S. Government Accountability Office** |
| **IT** | **Information Technology** |
| **NIST SP** | **National Institute of Standards and Technology’s Special Publication** |
| **OIG** | **Office of the Inspector General** |
| **OMB** | **U.S. Office of Management and Budget** |
| **OPM** | **U.S. Office of Personnel Management** |
| **SIEM** | **Security Information and Event Management** |

# TABLE OF CONTENTS

# I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by the American Postal Workers Union Health Plan (APWUHP).

The audit was conducted pursuant to FEHBP contract CS 1370; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act, enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our fourth audit of APWUHP's information technology (IT) general and application controls. The previous audits resulted in Report No. 1B-47-00-00-027, dated January 2, 2001; Report No. 1B-47-00-06-072, dated May 18, 2007; and Report No. 1B-47-00-11-044, dated June 27, 2011. All findings from the previous audits have been closed.

All APWUHP personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

# II. OBJECTIVES, SCOPE, AND METHODOLOGY

## OBJECTIVES

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in APWUHP's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to APWUHP's claims adjudication.

## SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of APWUHP's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of APWUHP's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by APWUHP to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Glen Burnie, Maryland.

The onsite portion of this audit was performed in February and March of 2017. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at APWUHP as of April 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by APWUHP. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable. In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed APWUHP's business structure and environment;
- Performed a risk assessment of APWUHP's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating APWUHP's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology 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 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

## COMPLIANCE WITH LAWS AND REGULATIONS

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

# III. AUDIT FINDINGS AND RECOMMENDATIONS

## A. SECURITY MANAGEMENT

Security management encompasses the policies and procedures that are the basis of APWUHP's overall IT security program. We evaluated APWUHP's ability to develop and maintain security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls. In addition, we reviewed APWUHP's human resources policies and procedures related to hiring, training, transferring, and terminating employees. Some of the controls we observed include:

**APWUHP has developed a thorough risk management methodology.**

- Documented policies and procedures that define the security management program;
- A thorough risk management methodology; and
- A process to create remediation plans to address weaknesses identified in risk assessments.

The following section documents one opportunity for improvement related to APWUHP's security management controls.

### 1) Specialized IT Training

APWUHP requires annual IT security and privacy awareness training for all employees. However, there are no formal requirements for individuals with specialized IT responsibilities to receive technical training specific to their job function.

NIST SP 800-53, Revision 4, explains that IT staff should receive "adequate security-related technical training specifically tailored for their assigned duties."

Failure to require role-based technical training for IT staff increases the risk that these individuals are not adequately prepared to address constantly evolving IT threats.

**Recommendation 1**

We recommend that APWUHP require routine job-specific training for employees with specialized IT security responsibility.

***APWUHP Response:***

***"APWUHP agrees with this recommendation and will review and revise our existing IT Training Policy to specify requirements for routine technical training tailored to each position that has specialized IT security responsibilities as part of the position."***

**OIG Comment:**

As a part of the audit resolution process, we recommend that APWUHP provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement applies to all subsequent recommendations in this audit report that APWUHP agrees to implement.

## B. ACCESS CONTROLS

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources. We examined the physical access controls of APWUHP's facilities and data centers. We also examined the logical controls protecting sensitive data on APWUHP's network environment and claims processing-related applications. The access controls observed during this audit include, but are not limited to:

- Policies and procedures for appropriately granting physical access to facilities;

- Policies and procedures for granting, changing, and removing access to systems and applications; and

- Multiple levels of approval for granting or changing access to systems and applications.

The following section documents opportunities for improvement related to APWUHP's access controls.

### 1) Data Center Physical Access

APWUHP's primary data center is located [redacted]. There are multiple controls that limit and monitor access to the space. [redacted]

[redacted]

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data.  Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

**Recommendation 2**

We recommend that APWUHP implement [redacted] and [redacted]

***APWUHP Response:***

***"APWUHP agrees with the recommendation to implement further controls [redacted] and plans implementation of these controls to be complete 4th Quarter, 2017."***

### 2) Routine Access Reviews

As noted above, APWUHP has implemented policies and procedures related to the provisioning of both physical and logical access.  However, APWUHP does not have procedures in place to periodically review active user accounts to ensure that both physical and logical access remains appropriate.  Our test work found that APWUHP had terminated employees without revoking the individual's access to APWUHP's physical facilities and information systems.

NIST SP 800-53, Revision 4, requires that "the organization . . . [r]eviews accounts for compliance with account management requirements . . ." on an organization defined frequency.

Failure to implement routine auditing of physical and logical access privileges increases the risk that an individual could gain unauthorized access to sensitive resources.

**Recommendation 3**

We recommend that APWUHP implement a process to routinely audit or review all active user accounts to ensure that both physical and logical access remains appropriate.

***APWUHP Response:***

***"APWUHP agrees with this recommendation and has partially satisfied compliance requirements by beginning auditing and remediation efforts. A formalized process and policy will be put in place by the Health Plan reflecting the processes established to satisfy this recommendation."***

**3)** [redacted]

[redacted]

[redacted]

[redacted]

**Recommendation 4**

We recommend that APWUHP implement [redacted].

***APWUHP Response:***

***"APWUHP agrees with the recommendation to implement [redacted]."***

### 4) Multi-factor Authentication for Remote Users

APWUHP uses a virtual private network to allow employees to remotely connect to its network. Although the connection is encrypted, multi-factor authentication is not enforced and users can connect with simply a username and password.

NIST SP 800-53, Revision 4, requires that systems with sensitive information implement "multifactor authentication for [remote] network access to privileged [and] . . . non-privileged accounts."

Failure to require multifactor authentication for remote users increases the risk that a malicious actor could gain unauthorized access to the internal network.

**Recommendation 5**

We recommend that APWUHP enforce multi-factor authentication for remote users to its information systems.

***APWUHP Response:***

***"APWUHP has since satisfied this recommendation. The Health Plan has completed remediation and implementation of multi-factor authentication for remote access to the Health Plan's network."***

**OIG Comment:**

In response to the draft audit report, APWUHP provided evidence that multifactor authentication is required for remote access. No further action is required.

## C. NETWORK SECURITY

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. We evaluated APWUHP's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit. We observed the following controls in place:

- A well-defined network topology documented with current and accurate diagrams;
- Preventive controls at the network perimeter; and
- Disk encryption.

The following section documents several opportunities for improvement related to APWUHP's network security controls.

### 1) [redacted]

[redacted] APWUHP has a project underway to address this issue.

[redacted]

[redacted]

[redacted]

**<u>Recommendation 6</u>**

We recommend that APWUHP complete its project to implement [redacted].

***<u>APWUHP Response:</u>***

***"APWUHP agrees with the recommendation. [redacted] is incorporated into APWUHP's network reorganization project to be completed by the Second Quarter of 2018."***

### 2) Firewall Configuration Standards and Audits

APWUHP has not formally documented a policy or standard that identifies the types of traffic allowed by the organization and the approved settings that are needed to harden firewalls within the network.

NIST SP 800-41, Revision 1, states that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies."

Without a documented firewall policy, APWUHP cannot effectively audit its firewall configuration because it does not have a baseline against which to compare the actual/current configuration. Failure to document an approved firewall policy and routinely audit the actual settings against this policy increases the risk that the firewall does not properly manage network traffic.

**Recommendation 7**

We recommend that APWUHP document a firewall policy and configuration standard.

***APWUHP Response:***

***"APWUHP agrees with the recommendation and is in process of completing documentation for firewall configuration standards."***

**Recommendation 8**

We recommend that APWUHP perform routine audits of its current firewall configurations against an approved firewall policy that is customized to its technical environment. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

***APWUHP Response:***

***"APWUHP agrees with this recommendation. APWUHP will include firewall configuration audits as part of its routine auditing and monitoring requirements and procedures."***

### 3) Network Access Controls

[redacted]

[redacted]

[redacted]

**Recommendation 9**

We recommend that APWUHP implement technical controls to [redacted]

***APWUHP Response:***

***"APWUHP agrees with the recommendation to implement further controls [redacted] and is currently looking at additional security controls to accompany those already in place for the Health Plan."***

### 4) Mobile Device Management

APWUHP is implementing a software product that controls the information available on mobile devices that connect to its network. However, not all mobile devices authorized to connect to the APWUHP network currently have the application installed.

NIST SP 800-53, Revision 4, identifies multiple controls that should be in place for mobile devices. These include: automated monitoring, encryption, and the ability to disable access. In addition it states that "The organization . . . establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices . . . ."

Failure to properly secure data on mobile devices increases the risk of improper disclosure of sensitive information.

**Recommendation 10**

We recommend that APWUHP fully implement its mobile device management capabilities on all devices.

***APWUHP Response:***

***"APWUHP has since satisfied this recommendation. The Health Plan has completed the process of fully implementing mobile device management on all devices connecting to the network."***

**OIG Comment:**

In response to the draft audit report APWUHP provided evidence that it implemented mobile device management software. No further action is required.

### 5) Security Information and Event Management

APWUHP is in the process of implementing a security information and event management (SIEM) system to better monitor its IT environment. However, only a limited number of network nodes are currently connected to the tool.

NIST SP 800-53, Revision 4, requires that an organization "Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information, and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization . . . ."

Automated security and event monitoring capabilities help recognize the relationship between correlated security events and reduces the risk that abnormal network activity or operations continue undetected.

**Recommendation 11**

We recommend that APWUHP finish configuring its SIEM tool and ensure all network devices are connected.

***APWUHP Response:***

***"APWUHP has since satisfied this recommendation. The Health Plan has completed the full configuration and implementation of a Security Information and Event Management System (SIEM)."***

**OIG Comment:**

In response to the draft audit report APWUHP provided evidence that it implemented a SIEM system. No further action is required.

### 6) Incident Response Testing

APWUHP does not have a policy that requires routine testing of its incident response plan.  Incident response activities are critical and time sensitive, and the response plan should be regularly tested and the results reviewed for any necessary changes or improvements.

**APWUHP does not have a policy that requires routine testing of its incident response plan**

NIST SP 800-53, Revision 4, states that "The organization tests the incident response capability for the information system . . . to determine the incident response effectiveness and documents the results."

Failure to test the incident response plan increases the risk that the plan will not properly function when necessary.

**Recommendation 12**

We recommend that APWUHP routinely test its incident response plan, and that any lessons learned are incorporated into the plan and policies.

***APWUHP Response:***

***"APWUHP agrees with the recommendation.  APWUHP will institute table top exercises in which the incident response plan will be reviewed, tested, and revised if necessary based on sample incidents and the effectiveness of response procedures that are currently in place."***

## D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard, and that updates or other changes are tracked and approved.  We evaluated APWUHP's management of the configuration of its computer workstations, servers, and databases.  Our review found the following controls in place:

- An approved configuration management policy;

- Documented system build guides; and

- A documented system change control process.

The sections below document areas for improvement related to APWUHP's configuration management controls.

### 1) Server Security Configuration Standards and Auditing

APWUHP has not documented formal security configuration standards for all operating platforms that are in use. A security configuration standard is an approved document that contains details on how security settings should be configured for specific operating platforms.

Furthermore, without a security configuration standard in place, APWUHP cannot effectively audit its systems' security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system . . . that reflect the most restrictive mode consistent with operational requirements . . . ." In addition, NIST SP 800-53, Revision 4, explains that an organization must develop, document, and maintain a current baseline configuration of the information system. Furthermore, FISCAM requires "Current configuration information should be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to establish system configuration standards increases the risk systems may not be configured in a secure manner.

**Recommendation 13**

We recommend that APWUHP document security configuration standards for all operating platforms and systems in its environment.

***APWUHP Response:***

***"APWUHP agrees with this recommendation. APWUHP currently has a configuration management policy and associated configuration process document for assets connected to***

***the network and are putting additional requirements and standards in place and reiterating in policy and process documentation."***

**<u>Recommendation 14</u>**

We recommend that APWUHP implement a process to routinely audit the configuration settings of its operating platforms to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 13 are in place.

***<u>APWUHP Response:</u>***

***"APWUHP agrees with this recommendation. As stated in response to Recommendation [13], APWUHP will have hardened configuration standards in place for the Health Plan."***

### 2) Patch Management

APWUHP has documented software patch management procedures. However, the vulnerability scanning test work performed during this audit indicated that for both operating platforms and applications within the APWUHP environment, there were various unapplied patches older than the grace period allowed by APWUHP's policy. The specific vulnerabilities that we identified will not be detailed in this report, but copies of the full scan reports were provided directly to APWUHP during the audit.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, requires that "The organization . . . [i]dentifies, reports, and correct information system flaws . . . [and] [i]nstalls security-relevant software and firmware updates" promptly.

Improving the patch management process would ensure that more vulnerabilities are remediated in a timely manner, further reducing the risk of malicious exploitation of vulnerabilities.

**<u>Recommendation 15</u>**

We recommend that APWUHP review its patch management policies and procedures and add additional controls to ensure the timely installation of patches and updates.

***<u>APWUHP Response:</u>***

***"APWUHP has since satisfied this recommendation. The Health Plan has reviewed and revised the existing Vulnerability Management Policy with regard to Patch Management to reflect more specific standards and requirements for installation of patches and updates as reported to system administrators from the Vulnerability Management System."***

**<u>OIG Comment:</u>**

In response to the draft audit report, APWUHP provided an updated policy on patch management. No further action is required.

### 3) Software Lifecycle

APWUHP leverages a variety of third-party software products in its technical environment. The vendors of these products typically publicize information related to the product's "end-of-life" support dates (i.e., dates when the vendor will no longer release security updates and patches). APWUHP's system inventory revealed multiple instances of servers running unsupported versions of operating platforms. APWUHP has indicated that it has plans to remove these unsupported systems.

NIST SP 800-53, Revision 4, requires that organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer . . . ." NIST SP 800-53, Revision 4, also states that "Unsupported components . . . provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components."

Failure to upgrade system software could result in information systems containing security vulnerabilities for which no remediation is available.

**<u>Recommendation 16</u>**

We recommend that APWUHP implement a methodology to ensure that information systems are upgraded to current versions before the end of vendor support.

***<u>APWUHP Response:</u>***

***"APWUHP has since satisfied this recommendation ensuring that information systems are upgraded to the current version prior to end of vendor support and processes are in place***

***for recording the [end of life] dates for inventory and reinforced in Configuration Management Policy."***

**OIG Comment:**

In response to the draft audit report APWUHP provided an updated policy and procedure for maintaining supported information systems. No further action is required.

**Recommendation 17**

We recommend that APWUHP upgrade or replace the unsupported operating platforms.

***APWUHP Response:***

***"APWUHP had since satisfied this recommendation. The Health Plan has upgraded/replaced all assets with unsupported operating platforms."***

**OIG Comment:**

In response to the draft audit report, APWUHP provided evidence that the unsupported operating platforms were either upgraded or removed from its network. No further action is required.

## E. CONTINGENCY PLANNING

Contingency planning includes the policy and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of APWUHP's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

- Disaster recovery plan and tests;
- Business continuity plan and tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." APWUHP has identified and prioritized the systems and resources that are critical to business operations, and have developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that APWUHP has not implemented adequate controls related to contingency planning.

## F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting APWUHP’s claims adjudication process. APWUHP adjudicates claims using a commercially available claims processing application. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, member enrollment, and provider debarment.

### 1) Application Configuration Management

We evaluated the policies and procedures governing application development and change control over APWUHP’s claims processing systems.

APWUHP uses vendor supported commercial software for claims adjudication and does not develop its own claims processing applications internally. APWUHP manages application configuration by coordinating changes with the vendor and testing changes at multiple steps in the process. A system has been implemented to track change requests, tickets, and testing throughout the change process.

Nothing came to our attention to indicate that APWUHP has not implemented adequate controls related to the application configuration management process.

### 2) Claims Processing

We evaluated the input, processing, and output controls associated with APWUHP’s claims adjudication process. We have determined the following controls are in place over APWUHP’s claims adjudication system:

**APWUHP has controls in place to track electronic claims through the adjudication process.**

- Adequate controls over the processing and output of claims;
- Quality assurance reviews of claims processing; and

- Tracking of electronic claims and files through the adjudication process.

The section below documents one opportunity for improvement related to the claims processing controls.

*Paper Claims Tracking*

Incoming paper claims arriving at APWUHP's mailroom are stored in an open work area after scanning.  While the area does have restrictions on access, the majority of employees involved in the claims adjudication process have access to this area.

NIST SP 800-53, Revision 4, requires that "The organization employs the principle of least privilege, allowing only authorized accesses for users . . . which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Failure to secure paper claims increases the risk that claims could be accessed by unauthorized individuals.

**Recommendation 18**

We recommend that APWUHP securely store paper claims throughout the claims adjudication process.

***APWUHP Response:***

***"The APWU Health Plan disagrees with this recommendation.  The paper claims referenced in this recommendation are located in the secure claims processing and customer service area.  Only authorized staff with controlled badge access are permitted in the secure area.  After the paper claims have been scanned and validated through the system, they are placed in a locked shredding bin for onsite shredding.  The APWU Health Plan has appropriate and adequate security controls in place, which manage the life cycle of paper claims throughout the claims adjudication process."***

**OIG Comment:**

We acknowledge that APWUHP has security controls in place protecting paper claims, but the concept of least privilege is not enforced.  NIST requirements for least privilege access mandate that controls be in place to limit individual access to only the resources needed to accomplish assigned responsibilities.  APWUHP's own policy states that employees "shall have access only to the protected health information that they need in order to perform their work-related duties" and that APWUHP is to both "appropriately supervise" and "fully document" this access. In this case, all employees in the claims processing and customer service areas can access any paper claim without accountability. At a minimum, we would expect that access to claims be restricted only to individuals whose job function requires access. As such, we continue to recommend that APWUHP securely store paper claims throughout the claims adjudication process.

### 3) Enrollment

We assessed APWUHP's procedures for managing its member enrollment data. Enrollment information is received electronically or in paper format (which is scanned and converted to digital) and is added into the enrollment database. The process includes controls to log the flow of enrollment data. APWUHP has resources dedicated to FEHBP enrollment and has additional resources on standby if needed to ensure that enrollment information is entered accurately and completely.

Nothing came to our attention to indicate that APWUHP has not implemented adequate controls over the enrollment process.

### 4) Debarment

APWUHP has documented procedures for reviewing provider files for debarred or suspended providers. The OPM OIG debarment list is downloaded monthly and prepared for uploading into APWUHP's claims system. Newly debarred providers are entered into the claims system and if a match is found on an existing provider then a hold is placed on claims for that debarred provider in the claims processing system. This process includes member notification, a 15-day grace period, and then denial of further claims.

Nothing came to our attention to indicate that APWUHP has not implemented adequate controls over the debarment process.

# Appendix

APWU
HEALTH PLAN
799 Cromwell Park Drive, Suites K-Z
Glen Burnie, MD 21061

American Postal Workers Union, AFL-CIO
Health Plan Department

Chief Operating Manager
[redacted]

Health Plan
Board of Directors

Mark Dimondstein
President

Deborah "Debby" Szeredy
Executive Vice President

Elizabeth "Liz" Powell
Secretary-Treasurer

Vance Zimmerman
Director, Industrial Relations

John L. Marcotte
Director, Health Plan

Clint Burelson
Director, Clerk Division

Steven G. Raymer
Director, Maintenance Division

Michael O. Foster
Director, MVS Division

Stephen R. Brooks
Director, Support Services Division

Sharyn M. Stone
Coordinator, Central Region

Mike Gallagher
Coordinator, Eastern Region

John H. Dirzius
Coordinator, Northeast Region

Kennith L. Beasley
Coordinator, Southern Region

Omar M. Gonzalez
Coordinator, Western Region

August 28, 2017

[redacted]
Auditor-In-Charge/Information Systems Audit Group
Office of Personnel Management
Office of Inspector General
Washington, DC 20415

Dear [redacted]:

Enclosed is the APWU Health Plan's response to the draft audit report 1B-47-00-17-018 dated June 27, 2017, issued by the Office of Inspector General. If after you review the enclosed responses, you are not in agreement with the Plan's stated position, we respectfully request that the APWU Health Plan be afforded the opportunity to meet with you or the OIG staff regarding those items on which we disagree. We believe that this will assure fair resolution of differences at the lowest cost to all parties and allow for the final report to be complete, accurate, fair and as free from errors of fact or omission as our combined efforts can make them.

Since the findings and recommendations in the draft report may change based on additional information provided, the APWU Health Plan reserves the right to review and modify its responses prior to the issuance of the final report.

I would like to reaffirm the American Postal Workers Union Health Plan's commitment to responsible administration of the FEHB Program. If you have any questions, please contact [redacted], CIO at the APWU Health Plan, at [redacted]

Cordially,

[redacted]

[redacted] Jr.
Chief Operating Manager

Attachments

cc: [redacted], Contracting Officer, Health Insurance Group II
[redacted], Contracts Specialist

# OPM-OIG Draft Audit Report 1B-47-00-17-018, APWUHP Response

## Recommendation 1

We recommend that APWUHP require routine job-specific training for employees with specialized IT security responsibility.

**APWUHP Response (Rec1):**
*APWUHP agrees with this recommendation and will review and revise our existing IT Training Policy to specify requirements for routine technical training tailored to each position that has specialized IT security responsibilities as part of the position.*

***[Redacted by OIG – not relevant to final report]***

## Recommendation 2

We recommend that APWUHP implement [redacted] and [redacted] [redacted].

**APWUHP Response (Rec2):**
*APWUHP agrees with the recommendation to implement further controls* [redacted] [redacted] *and plans implementation of these controls to be complete 4th Quarter, 2017.*

## Recommendation 3

We recommend that APWUHP implement a process to routinely audit or review all active user accounts to ensure that both physical and logical access remains appropriate.

**APWUHP Response (Rec3):**
*APWUHP agrees with this recommendation and has partially satisfied compliance requirements by beginning auditing and remediation efforts. A formalized process and policy will be put in place by the Health Plan reflecting the processes established to satisfy this recommendation.*

## Recommendation 4

We recommend that APWUHP implement [redacted] [redacted]

**APWUHP Response (Rec4):**
*APWUHP agrees with the recommendation to* [redacted] [redacted]

## Recommendation 5

We recommend that APWUHP enforce multi-factor authentication for remote users to its information systems.

**APWUHP Response (Rec5):**
*APWUHP has since satisfied this recommendation. The Health Plan has completed remediation and implementation of multi-factor authentication for remote access to the Health Plan's network.*
*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 6**

We recommend that APWUHP complete its project to implement internal firewalls at key locations on their network.

**APWUHP Response (Rec6):**

*APWUHP agrees with the recommendation. The firewall project is incorporated into APWUHP's network reorganization project to be completed by the Second Quarter of 2018.*

**Recommendation 7**

We recommend that APWUHP document a firewall policy and configuration standard.

**APWUHP Response (Rec7):**

*APWUHP agrees with the recommendation and is in process of completing documentation for firewall configuration standards.*

**Recommendation 8**

We recommend that APWUHP perform routine audits of its current firewall configurations against an approved firewall policy that is customized to its technical environment. Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

**APWUHP Response (Rec8):**

*APWUHP agrees with this recommendation. APWUHP will include firewall configuration audits as part of its routine auditing and monitoring requirements and procedures.*

**Recommendation 9**

We recommend that APWUHP implement technical controls to [redacted].

**APWUHP Response (Rec9):**

*APWUHP agrees with the recommendation to implement further controls* [redacted] *and is currently looking at additional security controls to accompany those already in place for the Health Plan.*

**Recommendation 10**

We recommend that APWUHP fully implement its mobile device management capabilities on all devices.

**APWUHP Response (Rec10):**

*APWUHP has since satisfied this recommendation. The Health Plan has completed the process of fully implementing mobile device management on all devices connecting to the network.*
*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 11**

We recommend that APWUHP finish configuring its SEIM tool and ensure all network devices are connected.

**APWUHP Response (Rec11):**

*APWUHP has since satisfied this recommendation. The Health Plan has completed the full configuration and implementation of a Security Information and Event Management System (SIEM).*
*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 12**

We recommend that APWUHP routinely test its incident response plan, and that any lessons learned are incorporated into the plan and policies.

**APWUHP Response (Rec12):**

*APWUHP agrees with the recommendation. APWUHP will institute table top exercises in which the incident response plan will be reviewed, tested, and revised if necessary based on sample incidents and the effectiveness of response procedures that are currently in place.*

**Recommendation 13**

We recommend that APWUHP document security configuration standards for all operating platforms and systems in its environment.

**APWUHP Response (Rec13):**

*APWUHP agrees with this recommendation. APWUHP currently has a configuration management policy and associated configuration process document for assets connected to the network and are putting additional requirements and standards in place and reiterating in policy and process documentation.*

**Recommendation 14**

We recommend that APWUHP implement a process to routinely audit the configuration settings of its operating platforms to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 14 are in place.

**APWUHP Response (Rec14):**

*APWUHP agrees with this recommendation. As stated in response to Recommendation 14, APWUHP will have hardened configuration standards in place for the Health Plan.*

**Recommendation 15**

We recommend that APWUHP review its patch management policies and procedures and add additional controls to ensure the timely installation of patches and updates.

**APWUHP Response (Rec15):**

*APWUHP has since satisfied this recommendation. The Health Plan has reviewed and revised the existing Vulnerability Management Policy with regard to Patch Management to reflect more specific standards and requirements for installation of patches and updates as reported to system administrators from the Vulnerability Management System.*

*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 16**

We recommend that APWUHP implement a methodology to ensure that information systems are upgraded to current versions before the end of vendor support.

**APWUHP Response (Rec16):**

*APWUHP has since satisfied this recommendation ensuring that information systems are upgraded to the current version prior to end of vendor support and processes are in place for recording the EOL dates for inventory and reinforced in Configuration Management Policy.*

*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 17**

We recommend that APWUHP upgrade or replace the unsupported operating platforms.

**APWUHP Response (Rec17):**
*APWUHP had since satisfied this recommendation. The Health Plan has upgraded/replaced all assets with unsupported operating platforms.*
*As this recommendation has been addressed, the Health Plan requests that the final audit report shows this as satisfied pending review of evidence provided.*

**Recommendation 18**
We recommend that APWUHP securely store paper claims throughout the claims adjudication process.

**APWUHP Response (Rec18):**
*The APWU Health Plan disagrees with this recommendation. The paper claims referenced in this recommendation are located in the secure claims processing and customer service area. Only authorized staff with controlled badge access are permitted in the secure area. After the paper claims have been scanned and validated through the system, they are placed in a locked shredding bin for onsite shredding. The APWU Health Plan has appropriate and adequate security controls in place, which manage the life cycle of paper claims throughout the claims adjudication process.*

APWU Health Plan appreciates the opportunity to provide these responses to your recommendations, and request that, where appropriate and with adequate redaction for security and confidentiality purposes, our responses be included in the Final Audit Report. If you have any questions or wish to see further documentation of APWU Health Plan's IT security systems and processes, please do not hesitate to contact us.

# 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