UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

June 27, 2011

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Follow-up Review of Information Systems General and Application Controls at American Postal Workers Union Health Plan (Report No. 1B-47-00-11-044)

The purpose of this memorandum is to communicate to you the findings and conclusions resulting from our follow-up review of information systems general and application controls conducted at American Postal Workers Union Health Plan (APWU). We initiated the review because of concerns regarding several instances of premature closure of recommendations stemming from information technology (IT) audits of insurance carrier systems.

The audit of APWU was scheduled because of the high risk associated with this health plan. A 2001 audit of this plan revealed significant weaknesses in their IT infrastructure. In 2007, we conducted an audit of APWU as a review of the information systems general and application controls as well as a re-evaluation of the 2001 recommendations.

As a result of our 2007 audit we made 46 recommendations for improvement in a wide range of business process and technical areas, including the overall IT security environment, business continuity, access controls, and application processing controls for APWU's claims adjudication system.

In January 2009, we discovered that all recommendations were closed by the Healthcare and Insurance Office (HIO) without proper documentation that corrective action had been completed. In accordance with OMB Circular A-50, and by longstanding custom, my office shares responsibility for audit resolution by reviewing corrective actions and rendering an opinion regarding their relevance and effectiveness at mitigating the weaknesses identified during our audits. In this case, we were not fully involved in this process. Closing audit recommendations without following the established processes not only allows health plans to avoid correcting significant weaknesses, but it also wastes limited audit resources expended to identify the weaknesses in the first place.

Executive Summary

The 2007 audit revealed that APWU had a very limited IT security program. We identified a variety of missing policies and procedures along with many technical vulnerabilities in the Plan's IT infrastructure. The audit report detailed 46 specific weaknesses in APWU's information systems general and application controls. The objective of this follow-up review was to evaluate the current status of each recommendation and determine which, if any, of the recommendations should be re-opened.

We concluded that APWU has made substantial progress in implementing a comprehensive IT security program, and that the Plan has fully addressed 41 of the 46 audit recommendations. However, five recommendations have not been fully implemented. We also issued one new recommendation resulting from the follow-up review. The unimplemented recommendations, and the one new recommendation we are making, from our follow-up review are outlined below:

- [redacted]
- [redacted]
- Medical Inconsistency Controls: [redacted] claims adjudication system processed and paid professional test claims with [redacted] inconsistencies and [redacted] inconsistencies.
- [redacted]
- [redacted] we believe this process should be automated.
- Special Investigations and Fraud: All components of a comprehensive fraud and abuse program as required by OPM Carrier Letter 2003-23 are not currently implemented at APWU.

Background

Audit report 1B-47-00-06-072 was issued on May 18, 2007 with 46 audit recommendations. APWU subsequently provided the HIO with seven quarterly status reports detailing its progress in implementing the recommendations. HIO responded to each quarterly status report with a letter indicating which audit recommendations were being closed that quarter. On January 12, 2009, HIO sent a final closure letter to APWU indicating that all 46 recommendations were closed. However, 22 of the recommendations were closed based solely on a description of

APWU's plans to address the weakness, even though no actual evidence was provided to indicate that the recommendation had been addressed.

The issuance of the HIO closure letter created the possibility that APWU would halt its ongoing efforts to remediate the weaknesses identified during the audit. As a result of this concern, we initiated this follow-up review to determine the current status of the original audit recommendations and reopen any that had still not been completed.

Scope and Methodology

The scope of this review was limited to the business processes where weaknesses were identified during the original audit, including:

- Entity-wide Security;
- Access Controls;
- Application Development and Change Control;
- System Software;
- Service Continuity; and
- Application Controls.

In conducting this review we gathered documentation and conducted interviews related to remediation activity APWU has completed to address our original audit recommendations. Various laws, regulations, and industry standards were used as a guide to evaluate the APWU control structure. This criteria includes, but is not limited to:

- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's Federal Information System Controls Audit Manual;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and
- HIPAA Act of 1996.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a review, the documentation, reporting, and quality control standards are not as rigorous.

Review Follow-up

In accordance with Office of Management and Budget (OMB) Circular A-50 and/or Public Law 103-355, all findings must be resolved within six months of the date of this report. In order to ensure findings are resolved within the required six-month period, we ask that the Healthcare and Insurance Office (HIO) respond directly to the Office of the Inspector General (OIG) within 90 days of the date of the report advising us whether they agree or disagree with the findings and recommendations. As stated in OMB Circular A-50, where agreement is indicated, the HIO should describe planned corrective action. If the HIO disagrees with any of the findings and recommendations, we need them to explain the reason for the disagreement and provide any additional documentation that would support their opinion.

Since this office exercises oversight regarding the progress of corrective actions, we also request that the HIO provide the OIG a report within six months describing corrective action taken. If the corrective action has not been completed, we also ask that the HIO continue to provide us with a report on the status of corrective action every March and September thereafter until action has been completed.

Results

The following sections outline the results of our follow-up review of information systems general and application controls at APWU.

A. Entity-wide Security

We evaluated the adequacy of APWU's ability to manage risk, develop security policies, assign security-related responsibilities, and monitor the effectiveness of various system-related controls.

1. Enterprise Security Program

APWU had developed a series of information technology (IT) security policies and procedures that comprised its enterprise security program. However, we determined that APWU had not adequately maintained all policies on its intranet, not all policies were being enforced, and individuals with significant security responsibilities were not always familiar with these policies.

a. 2007 Recommendation 1

We recommend that APWUHP update its security policies on its intranet, properly enforce them, and ensure that individuals with IT security responsibilities are familiar with these policies. A formal policy requiring periodic reviews and updates of security policies should also be established.

2007 APWU Response:

"The APWU Health Plan does maintain an Emergency Termination Checklist for all involuntary terminations. This checklist was provided to the Office of Inspector General's auditors along with the procedures. It is APWU Health Plan Information System's responsibility to complete and retain this check list and not the Human Resource Department which is why they may have been unfamiliar with the forms in question.

The Health Plan updates our security policies and procedures on our Intranet application, RoboInfo. A Standard Operating Procedure was written to provide guidance for reviewing and updating security policies and procedures on a bi-annual basis, or as needed when new rules or regulations are published and to train staff appropriately. See Attachment 1A for the updated Standard Operating Procedures."

2011 Status:

We confirmed that APWU has sufficiently updated its security policies and made them readily available on its intranet; this recommendation is closed.

2. Risk Assessment

APWU's risk assessment methodology did not appear to identify, evaluate, or provide mitigating options for threats and vulnerabilities to its information systems.

a. 2007 Recommendation 2
We recommend that APWUHP update its risk assessment policy to include steps to identify, evaluate, and mitigate threats and vulnerabilities to its systems.

2007 APWU Response:
"The APWU Health Plan is currently reviewing the NIST 800-30 'Risk Management Guide for Information Technology Systems' and will be updating our risk assessment to identify, evaluate, and provide mitigation options for threats and vulnerabilities to their current information system and applications. It is the Health Plan's goal to complete this assessment during the first quarter of 2007."

2011 Status:
We confirmed that APWU has implemented an adequate risk assessment methodology; this recommendation is closed.

3. Incident Response

APWU had not properly defined the organizational structure of individuals responsible for handling IT security incidents. In addition, employees with incident response duties received no formal training related to this responsibility.

a. 2007 Recommendation 3
We recommend APWUHP implement a formal, documented security management structure that outlines the responsibility and authority of APWUHP personnel charged with responding to IT security incidents.

2007 APWU Response:
"The APWU Health Plan will create and implement formal documented Security Management Procedures and communicate those procedures to the appropriate personnel."

2011 Status:
We confirmed that APWU has implemented a security management structure that details the personnel responsible for responding to IT security incidents; this recommendation is closed.

b. 2007 Recommendation 4
We recommend APWUHP create a policy requiring adequate training for individuals responsible for responding to security incidents.

2007 APWU Response:
"The APWU Health Plan will create a policy to address the training for individuals responsible for responding to security incidents."

2011 Status:
We confirmed that APWU has implemented an IT Training and Development policy; this recommendation is closed.

4. Background Reinvestigations

APWU conducted thorough background investigations on all individuals hired by the Plan. However, APWU did not conduct periodic reinvestigations of its employees.

a. 2007 Recommendation 5
We recommend that APWUHP implement a policy requiring periodic background reinvestigations on all Health Plan employees.

2007 APWU Response:
"The APWU Health Plan has investigated this recommendation and will implement criminal background reinvestigations."

2011 Status:
We confirmed that APWU has implemented a periodic background reinvestigations policy; this recommendation is closed.

5. Training

Employees did not receive continuing periodic training or professional development courses to ensure that an employee's skills are maintained for their job responsibilities.

a. 2007 Recommendation 6
We recommend that APWUHP develop and implement a formal training program that requires periodic training for all employees.

2007 APWU Response:
"Per the Security Reminders Standard Operating Policy & Procedures provided to auditors, Health Plan staff receive refresher training on HIPAA Security procedures during annually scheduled workforce benefits training each year. In addition, any changes that need to be immediately addressed are handled via business unit meetings or formalized training sessions as needed."

2011 Status:
We confirmed that APWU has implemented a formal training program; this recommendation is closed.

B. Access Controls

We reviewed and evaluated the effectiveness of the access control policies, procedures, and techniques APWU had in place to help ensure that unauthorized physical or logical access to sensitive resources are both minimized and actively monitored.

1. Data Center Controls

While APWU's data center was physically secure from the outside world, employees with no responsibilities related to the computer equipment in the data center were granted access. In addition, guests to the data center were not required to sign a log detailing their entrance to the data center, the purpose of their visit, and their escort. We also found that APWU had not implemented any video monitoring capabilities in the data center, or at its entrances.

a. 2007 Recommendation 7
We recommend that APWUHP limit access to the data center to management and maintenance personnel, and to those with responsibilities that require physical access to computing resources in the data center.

2007 APWU Response:
"The APWUHP does limit access to the Data Center and as suggested in Recommendation 7, have restricted access for the Insertamax Operators."

2011 Status:
We confirmed that APWU has limited access to the data center; this recommendation is closed.

b. 2007 Recommendation 8
We recommend that APWUHP maintain a log of all visitors that access its data center.

2007 APWU Response:
"The APWU Health Plan has considered this recommendation and has determined that with the installation of the video monitors (see Recommendation 9 response below) in the computer room, limited access by the security doors and requiring outside vendors to sign-in and be escorted when they enter the building, that we have adequate controls for the data center."

2011 Status:
We confirmed that APWU logs all visitor access to the data center; this recommendation is closed.

c. 2007 Recommendation 9
We recommend that APWUHP implement [redacted] in its data center.

2007 APWU Response:
"The APWU Health Plan has entered into a contract with [redacted]

2011 Status:
As of May 2011 APWU has installed [redacted] within the data center. However, we observed that [redacted]

2011 Recommendation 1:
We recommend that APWU enhance [redacted]

2. Security of Check Stock and Printed Checks

Pre-printed check stock and printed checks were stored in an unsecured location.

a. 2007 Recommendation 10
We recommend that APWUHP secure pre-printed check stock within its data center.

2007 APWU Response:
"The APWU Health Plan has reviewed the recommendation and feel we have adequate controls over the check stock within the data center. The check stock is stored within the data center, which has limited access. Only individuals authorized to enter the data center have access and any other individual entering the data center is escorted. The APWU Health Plan's contract with the bank calls for a positive pay verification by the bank prior to cashing checks. The APWU Health Plan sends the bank a daily check register of all claim checks issued. If someone were to attempt to type their own check, the bank would reject the transaction. All checks are accounted for in a reconciliation process between Computer Operation and Accounting. Additionally, with the installation of the video cameras in the data center, one of these cameras will be able to monitor the blank preprinted check stock."

2011 Status:
We confirmed that APWU has secured the pre-printed check stock within the data center; this recommendation is closed.

b. 2007 Recommendation 11
We recommend that APWUHP adjust its procedures for mailing printed checks so that the checks are never left unattended in an insecure area.

2007 APWU Response:
"The APWU Health Plan has reviewed this recommendation and determined that there are adequate controls in place. [redacted] *Additionally, there*

is the positive pay processes with the bank and as back up, the member is mailed an explanation of benefits of what was paid."

2011 Status:
We confirmed that APWU has adjusted its procedures to appropriately secure printed checks prior to mailing; this recommendation is closed.

3. Application Access Controls

Controls to prevent unauthorized logical access to APWU's information systems were not adequately implemented. Specifically, APWU did not have a corporate password policy implemented, which was an outstanding recommendation from 2001.

Passwords were assigned by the system administrator and were known by at least three individuals before being provided to the user. Each user's password was stored in hard copy by the Plan's HIPAA specialist. Passwords were not subject to any complexity requirements and there were no controls implemented to prevent unlimited login attempts.

a. 2007 Recommendation 12
We recommend that APWUHP implement a corporate password policy that meets the requirements of FISCAM and NIST SP 800-14. At a minimum, the policy should address minimum password lengths, the use of alphanumeric and special characters, routine password changes and reuse of passwords.

2007 APWU Response:
"Currently, security and password controls are handled on the application level. Each application has different password requirements and do not allow for the user to choose, or change their password, nor do they possess the ability to lock accounts after a pre-determined number of failed login attempts. The Health Plan will prepare business requirements and functional specifications to present to the vendors for each application in order to put together a uniform corporate password policy that meets the requirements of FISCAM and NIST SP 800-14 guidelines. These business requirements and functional specifications will be presented to the vendor during the first quarter of 2007."

2011 Status:
We confirmed that APWU has implemented a sufficient corporate password policy; this recommendation is closed.

b. 2007 Recommendation 13
We recommend that APWUHP adjust its procedures for issuing users' initial passwords so that only that individual knows his/her password. This can be accomplished by allowing users to set their own passwords, or by forcing users to change their assigned password on first use.

2007 APWU Response:
"Currently, security and password controls are handled on the application level. Each application has different password requirements and do not allow for the user to choose, or change their password, nor do they possess the ability to lock accounts after a pre-determined number of failed login attempts. The Health Plan will prepare business requirements and functional specifications to present to the vendors for each application in order to put together a uniform corporate password policy that meets the requirements of FISCAM and NIST SP 800-14 guidelines. These business requirements and functional specifications will be presented to the vendor during the first quarter of 2007."

2011 Status:
We confirmed that APWU has implemented system settings to mandate password changes upon initial sign-on; this recommendation is closed.

c. 2007 Recommendation 14
We recommend that APWUHP improve the password controls for the applications discussed in this section to meet the requirements of the corporate password policy.

2007 APWU Response:
"Currently, security and password controls are handled on the application level. Each application has different password requirements and do not allow for the user to choose, or change their password, nor do they possess the ability to lock accounts after a pre-determined number of failed login attempts. The Health Plan will prepare business requirements and functional specifications to present to the vendors for each application in order to put together a uniform corporate password policy that meets the requirements of FISCAM and NIST SP 800-14 guidelines. These business requirements and functional specifications will be presented to the vendor during the first quarter of 2007."

2011 Status:
[redacted]. This is in direct violation of the Corporate Password Policy.

2011 Recommendation 2:
We continue to recommend that APWU improve the password controls to meet the standards established within the corporate password policy.

d. 2007 Recommendation 15
We recommend that APWUHP configure the applications to lock accounts after a pre-determined number of failed login attempts.

2007 APWU Response:
"Currently, security and password controls are handled on the application level. Each application has different password requirements and do not allow for the user to choose, or change their password, nor do they possess the ability to lock accounts after a pre-determined number of failed login attempts. The Health Plan will prepare business requirements and functional specifications to present to the vendors for each application

in order to put together a uniform corporate password policy that meets the requirements of FISCAM and NIST SP 800-14 guidelines. These business requirements and functional specifications will be presented to the vendor during the first quarter of 2007."

2011 Status:
We confirmed that APWU has implemented the system changes to lock accounts after failed login attempts; this recommendation is closed.

4. Access Monitoring

APWU did not adequately monitor access to three systems critical to claims processing activities and we found that activity is not monitored for APWU employee workstations and the data entry application.

In addition, APWU's configuration of its virtual private network (VPN) software did not enable the logging of user activity.

a. 2007 Recommendation 16
We recommend that APWUHP routinely monitor access to its information systems in accordance with its "Login Monitoring" policy.

2007 APWU Response:
"Currently, the Health Plan is unable to monitor activity or log-in attempts at the application level. The Health Plan will prepare business requirements and functional specifications to present to the vendors for each application that meets the requirements of the NIST 800-12 and the HIPAA Security Rule 164.308(a)(1)(ii)(D) guidelines. These business requirements and functional specifications will be presented to the vendors during the first quarter of 2007.

2011 Status:
We confirmed that APWU has implemented procedures that correspond with the Login Monitoring policy; this recommendation is closed.

b. 2007 Recommendation 17
We recommend that APWUHP enable the auditing capabilities of its VPN server to monitor remote access activity.

2007 APWU Response:
"The APWU Health Plan has currently requested proposals for implementing Firewall/VPN logging."

2011 Status:
We confirmed that APWU has implemented the appropriate system changes to enable VPN server auditing; this recommendation is closed.

5. Intrusion Detection

APWU had not implemented any intrusion detection systems on its network or individual workstations.

a. 2007 Recommendation 18
We recommend that APWUHP implement some form of intrusion detection capability.

2007 APWU Response:
"The APWU Health Plan has requested proposals for implementing Intrusion Detection."

2011 Status:
We confirmed that APWU implemented intrusion detection; this recommendation is closed.

6. E-mailing Personal Health Information (PHI)

APWU's "E-mailing PHI" policy did not provide adequate guidance for properly securing PHI sent over email.

a. 2007 Recommendation 19
We recommend that APWUHP update its data transmission policy and procedures to ensure that PHI transmitted over e-mail is properly encrypted.

2007 APWU Response:
"Although the HIPAA regulations do not require that e-mail be encrypted, the Health Plan continues to look at additional technology to ensure the security of electronic PHI when e-mail is transmitted outside the organization's systems and applications."

2011 Status:
We confirmed that APWU has updated its data transmission policy and procedures to address the secure transmission of PHI; this recommendation is closed.

7. Internet Usage

APWU's "Information Technology Policy" did not address the appropriate use of the Internet and acceptable web browsing practices.

Furthermore, we determined that APWU did not utilize any Internet monitoring or filtering software.

a. 2007 Recommendation 20
We recommend that APWUHP implement an Internet use policy that describes, in detail, allowable web browsing practices by Plan employees.

2007 APWU Response:
"On December 12, 2006, the APWU Health Plan issued an Information Technology – Security Policy that addresses access to APWU Health Plan's equipment, software, information transmission and Internet. See Attachment 20A."

2011 Status:
We confirmed that APWU has implemented an Internet use policy; this recommendation is closed.

b. 2007 Recommendation 21
We recommend that APWUHP implement some form of Internet filtering software to enforce the Plan's Internet use policy.

2007 APWU Response:
"The APWU Health Plan is currently pursuing proposals from our vendors for implementing Content Management/Filtering."

2011 Status:
We confirmed that APWU has implemented Internet filtering software; this recommendation is closed.

8. Firewall Utilization

We determined that APWU's utilization of firewalls in its network environment could be improved. [redacted] contracted to perform the original configuration of the firewall ruleset, but no internal or third party reviews of the firewall ruleset have been conducted since its implementation and changes made to the ruleset are not logged.

[redacted].

a. 2007 Recommendation 22
We recommend that APWUHP periodically review its firewall rulesets and evaluate their effectiveness in controlling current security threats.

2007 APWU Response:
"The APWUHP will monitor, log changes and periodically review rule sets."

2011 Status:
We confirmed that APWU periodically reviews its firewall rulesets with regard to current security threats; this recommendation is closed.

b. 2007 Recommendation 23
We recommend that APWUHP research the costs, benefits, and feasibility of [redacted].

2007 APWU Response:
"The APWU Health Plan reviewed this recommendation and found that Health Plan users are [redacted], the costs associated [redacted] is not a cost effective security measure at this time. The Plan will continue to evaluate this recommendation as other changes are made."

2011 Status:
APWU has not implemented the recommended [redacted] and has formally accepted all associated risk. APWU stated that *"The APWU Health Plan has reviewed this recommendation again to see if [redacted] is feasible. The costs associated with [redacted] is not a cost effective security measure at this time. The Health Plan will continue to evaluate this recommendation as other enhancements and modifications are made to our technical infrastructure."*

This recommendation is closed based on APWU's risk acceptance, but we advise APWU to continue to evaluate the feasibility and benefits of implementing the recommendation.

C. Application Development and Change Control

We reviewed the APWU application development and change control methodology to determine whether it included the following features: a process for authorizing processing features and programming modifications; a change control process with testing standards and practices; approval methods for the implementation of newly developed or revised software; and controls over the use of application-related source code and program libraries.

1. Change Control Procedures

APWU's "Application Change Control manual" did not reflect the current environment for [redacted].

a. 2007 Recommendation 24
We recommend that APWUHP update the "Application Change Control Manual" to reflect its current operating environment. We also recommend that APWUHP ensure that the updated application development and change control policies and procedures are effectively communicated to the appropriate staff members.

2007 APWU Response:
"The APWU Health Plan is in the process of reviewing and updating the "Application Change Control manual" to reflect the current operating environment. Once the document has been fully updated, it will be communicated to the appropriate staff."

2011 Status:
We confirmed that APWU has sufficiently updated the change control policies and procedures; this recommendation is closed.

2. Testing Modifications

APWU's procedures for testing the [redacted] claims processing application were not adequate to ensure the continuing functionality of all system components.

a. 2007 Recommendation 25
We recommend that APWUHP develop a testing methodology that includes test cases for all major functions (modules) of the claims processing system. The test plans should also include reusable test data with verifiable expected results. Each time the system is modified, APWUHP should compare its expected results to those obtained during the testing exercise.

2007 APWU Response:
"The APWU Health Plan agrees with the recommendation to institute regression testing into the Health Plan's testing methodology."

2011 Status:
We confirmed that APWU has developed and implemented a claims processing testing methodology; this recommendation is closed.

D. System Software

We evaluated APWU's configuration and management of the [redacted] operating platform that houses the Plan's claim processing system.

1. Accessing System Software

Two [redacted] software administrators would occasionally log into the [redacted] root account directly instead of using their personal [redacted] accounts. This practice reduced the accountability of administrators for their system activity, as it was impossible to tell which individual was logged into the root account. A better practice is for administrators to log into their personal account and then execute the "switch user" command to access the root account when needed. This approach results in an audit trail of the administrator's activity.

a. 2007 Recommendation 26
We recommend that APWUHP implement a policy requiring system software administrators to always log into their personal [redacted] accounts, and use the "switch user" command to perform root functions.

2007 APWU Response:
"The APWU Health Plan agrees that creating a policy requiring the system software administrators to always log into their [redacted] accounts first and then use the [redacted]

to perform root functions, would allow better monitoring of which users gained root access. APWU Health Plan is in the process of drafting this policy."

2011 Status:
We confirmed that APWU has implemented the recommended system software administrators login policy; this recommendation is closed.

2. [redacted]

We reviewed the [redacted] system configuration file and determined that two s[redacted] hat may not have a business justification for being utilized.

a. 2007 Recommendation 27
We recommend that APWUHP research the purpose of the [redacted]. If no business purpose can be found, we recommend that APWUHP consider disabling [redacted]. If a business purpose is found, we recommend that APWUHP research secure alternative [redacted] that can perform the same function.

2007 APWU Response:
"The APWU Health Plan is researching the business purpose of the [redacted] being active in the [redacted]. So far, three production jobs have been identified requiring the [redacted] to be active. The initial result of turning off the [redacted] resulted in the failure of these three production jobs. We are continuing research to find additional production jobs and ways to limit use of [redacted]."

2011 Status:
We confirmed that APWU has researched and determined that a business necessity does exist for the use of these [redacted]. The risk associated with the continued use of these system services has been accepted by APWU; this recommendation is closed.

3. System Software Change Control

APWU does not maintain a log of past changes to its system software.

a. 2007 Recommendation 28
We recommend that APWUHP maintain a log of all changes to its system software.

2007 APWU Response:
The APWU Health Plan will maintain a log of all changes.

2011 Status:
We confirmed that APWU has implemented a system change control log; this recommendation is closed.

E. Service Continuity

We reviewed APWU's service continuity program to determine if (1) procedures were in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan existed to recover critical operations should interruptions occur.

1. Identifying Critical Operations and Resources

APWU had identified the systems that are critical to continuing business operations. However, the Plan had not adequately identified the priority in which these systems should be restored in a disaster recovery situation.

a. 2007 Recommendation 29
We recommend that APWUHP establish the priority in which each of its systems be restored in an emergency recovery situation.

2007 APWU Response:
"The Health Plan has updated its Disaster Recovery Plan to include the priority in which each of its systems is to be restored."

2011 Status:
We confirmed that APWU has prioritized the systems to be restored in an emergency recovery situation; this recommendation is closed.

b. 2007 Recommendation 30
We recommend that APWUHP identify the specific resources that support each of its systems.

2007 APWU Response:
"The Health Plan has updated its Disaster Recovery Plan to include specific resources to support each of its systems."

2011 Status:
We confirmed that APWU has identified the system specific resources; this recommendation is closed.

2. Disaster Recovery Plan

APWU's disaster recovery manual contained the majority of elements suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems." However, several critical elements were missing from the manual regarding alternate team members, travel arrangements, and contact information.

a. 2007 Recommendation 31
We recommend that APWUHP update its disaster recovery plan to include the missing elements discussed in the section above.

2007 APWU Response:
"The Health Plan is currently in the process of selecting and contracting with a new disaster recovery vendor. The Disaster Recovery Plan will be updated appropriately once the vendor has been selected and a new contract executed. In addition, the DR Plan will be updated with current contact information and updated team members. This will be completed during the first quarter of 2007."

2011 Status:
We confirmed that APWU has updated its disaster recovery plan; this recommendation is closed.

3. Business Continuity Testing

APWU had implemented a business continuity plan, but it had not been tested.

a. 2007 Recommendation 32
We recommend that APWUHP test its business continuity plan at least annually.

2007 APWU Response:
"The Health Plan conducted several system recovery tests during 2006. The written results of the last two tests were supplied to the auditors. Once the Disaster Recovery Plan is updated and a new vendor is chosen during the first quarter of 2007, the Health Plan will conduct further system recovery tests and will plan at least one full tabletop test of the plan during 2007."

2011 Status:
We confirmed that APWU has conducted an annual test of their business continuity plan; this recommendation is closed.

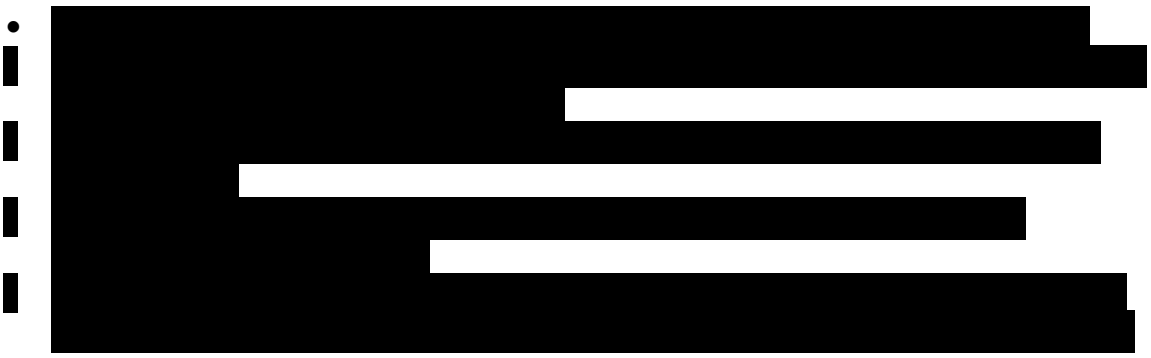
F. Application Controls

We evaluated the input, processing, and output controls associated with APWU's [redacted] claims processing system. During this process we reviewed the policies and procedures adopted by APWU to help to ensure that 1) there are controls over the inception of claims data into the system; 2) the data received comes from the appropriate sources; and 3) the data is entered into the claims database correctly.

1. Processing Controls

A test of the [redacted] system revealed several weaknesses in APWU's claims processing controls, including:

- [redacted]



a. 2007 Recommendation 33
We recommend that APWUHP expand [redacted] clinical edits for professional claims to account for the medical inconsistencies stated above. We also recommend that APWUHP take the necessary steps to ensure that these clinical edits are also applied to hospital claims.

2007 APWU Response:
"The Health Plan agrees we need to minimize [redacted] s and has reported this problem to the claims software vendor [redacted] to correct the [redacted] issue that has been identified. Currently, the software editing product used [redacted]) in the claims system, [redacted] does not accommodate editing for hospital claims. The Health Plan will take steps to investigate a product that will accommodate editing on hospital claims."

2011 Status:
We submitted several professional test claims into APWU's [redacted] claims processing test system to evaluate the effectiveness of the system's clinical edits. The [redacted] system processed and paid a [redacted] In addition, several hospital test claims were submitted into the system. A hospital test claim for [redacted] did not encounter the expected clinical edit. [redacted]

[redacted] increases the risk that claims can still be processed inaccurately and generate erroneous payments, increasing the costs to the FEHBP.

2011 Recommendation 3:
We continue to recommend that APWU expand [redacted] clinical edits for professional and hospital claims to account for the medical inconsistencies stated above.

b. 2007 Recommendation 34
We recommend that APWUHP implement the proper technical controls to its claims processing system to ensure that providers are only paid for services for which they are covered.

2007 APWU Response:
"The Health Plan has controls in place, such as claims audits and Ingenix sends a list of providers which are flagged in the system as fraudulent in order to ensure providers are only paid for services for which they are covered."

2011 Status:
We submitted a professional test claim into APWU's [redacted] claims processing test system to evaluate the effectiveness of the system's [redacted] The [redacted] system processed and paid a [redacted] test claim for a [redacted] In addition a hospital test claim was processed and paid for a [redacted] These tests revealed the potential for APWU to erroneously pay claims for services [redacted].

APWU personnel explained that [redacted]

The lack of adequate [redacted] within the [redacted] application increases the risk that claims can still be processed inaccurately, generating erroneous payments, and thereby increasing the costs to the FEHBP.

2011 Recommendation 4:
We continue to recommend that APWU implement the proper technical controls to its claims processing system to ensure that [redacted]

c. 2007 Recommendation 35
We recommend that APWUHP implement the appropriate controls to ensure that only providers in the [redacted] provider file are paid, and that new providers are flagged for review before being added to the system.
2007 APWU Response:
"The APWU Health Plan will satisfy this requirement in conjunction with implementation of the National Provider Identifier. Only providers that have valid identification numbers from CMS will be considered for payment. New providers without a provider identification number will be flagged for review."

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

d. 2007 Recommendation 36
We recommend that APWUHP implement the necessary technical controls to identify and process workers' compensation and coordination of benefits claims in accordance with its FEHBP contract.

2007 APWU Response:
"Due to the time it takes for the Office of Workers' Compensation to make a determination and the fact that the APWU Health Plan members should be afforded medical services for their injury, the APWU Health Plan has been reluctant to out right deny possible workers' compensation claims. Instead the claims are flagged along with subrogation claims. The accident code used on these claims would be picked up by the subrogation programs to follow-up with a questionnaire and legal review."

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

e. 2007 Recommendation 37
We recommend that APWUHP implement the necessary technical controls to its claims processing system to ensure that assistant surgeon claims are processed and paid correctly.

2007 APWU Response:
"The APWU Health Plan agrees with this recommendation and will have the capability to handle assistant surgeon correctly when the claims system vendor, [redacted], completes enhancement 6.66."

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

2. Debarment

The provider files for APWU's [redacted] claims processing system did not contain information to properly identify/flag all FEHBP debarred providers. In addition, several FEHBP debarred providers were not found in the provider file at all, and could potentially be added to the system automatically without being flagged for review.

We also submitted a series of test claims to test whether [redacted] performs the following actions in accordance with the benefit structure's guidelines: 1) pay the first claim submitted for an enrollee receiving services from a debarred provider, 2) pay subsequent claims submitted within 15 days of the enrollee being notified for the debarment, and 3) deny claims received later than 15 days after the enrollee is notified of the debarment. The system denied claims for all three situations.

a. 2007 Recommendation 38
We recommend that APWUHP update [redacted] provider file with the current complete list of FEHBP debarred providers (including those not previously in the system), and continue to update the file as new debarment lists are released by the OPM OIG.

2007 APWU Response:
"This issue was corrected prior to the Office of Inspector General exit conference. The process is working correctly as debarment lists are issued and the Health Plan updates the files in the claims adjudication system, [redacted]

2011 Status:
The OIG has confirmed that the recommended changes to the debarment process have been implemented; this recommendation is closed.

b. 2007 Recommendation 39
We recommend that APWUHP implement the necessary controls to ensure that claims for debarred providers are processed in accordance with the OIG Guidelines.

2007 APWU Response:
"The Health Plan agrees and has taken the necessary steps to comply with the OIG guidelines. An enhancement request (number 6.68) is currently being worked on by the software vendor, RAM Technologies."

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

3. OBRA90/DRG Transfers

APWU's claims adjudication process did not adequately address all required fields of OBRA90 claims sent to the CMS PRICER program. The APWU "Procedures for Data Input into Pricer" do not instruct claims examiners in how to address the discharge status code field when pricing an OBRA90 claim.

a. 2007 Recommendation 40
We recommend that APWUHP update its policies and procedures to ensure that claim data is entered in the CMS PRICER program accurately and completely. These policies and procedures should be in accordance with CMS and/or OPM guidance.

Once the policies and procedures have been implemented, we recommend that APWUHP train the claims examiners on these updated policies and procedures.

2007 APWU Response:
"As a result of this audit finding, the APWU Health Plan opened a problem report with our software vendor, RAM. The CMS Pricer Program is integrated in the claims

processing system and the process to price a claim is only recognizing status code '2' (discharge/transferred for inpatient care), and it should recognize all discharge status codes."

2011 Status:
The OIG has confirmed that the recommended policies and procedures have been implemented; this recommendation is closed.

4. OBRA 90/DRG Pre-certification Penalty

APWU's claims processing system did not apply the $500 pre-certification penalty on any of the OBRA90 test claims processed during the 2007 audit.

a. 2007 Recommendation 41
We recommend that APWUHP implement the necessary claims processing system changes to ensure that pre-certification rules are properly enforced for all FEHBP claims.

2007 APWU Response:
"Currently, DRG claims are priced and processed directly in [redacted] *There have been no situations identified where the penalty was not taken when it should have been. Controls are in place within the unit to escalate any claims to the Supervisor where the system is not applying the penalty correctly."*

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

5. Medicare Part B

APWU was incorrectly paying some OBRA90 claims in which the patient has Medicare Part B. Processors used the actual billed charges instead of the DRG equivalent amount when paying this claim, which is against OPM guidelines.

a. 2007 Recommendation 42
We recommend that APWUHP revise its procedures to use the DRG equivalent amount even if the priced amount is greater than the billed amount.

2007 APWU Response:
"The Health Plan agrees with the recommendation and has taken steps to correct the internal procedures. The Plan now uses the DRG equivalent amount that the [redacted] *Pricer calculated even if more than the charge."*

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

6. PRICER Input

The [redacted] system only transmitted the last five digits of the total charges to the CMS PRICER program, resulting in the incorrect pricing of OBRA90 claims.

a. 2007 Recommendation 43
We recommend that APWUHP implement the proper technical controls to ensure that OBRA90 claims with total charges of $100,000 or more are priced correctly using the CMS PRICER program.

2007 APWU Response:
"When the OIG reviewed these claims, the CMS Pricer process was not integrated into the claims adjudication system. Now the CMS Pricer is integrated and operating correctly. APWUHP validated that claims with total charges of $100,000 or more are priced correctly using the Pricer program. We will continue to monitor pricing results when updates are done to the Pricer program."

2011 Status:
We confirmed that the recommended system modifications have been implemented; this recommendation is closed.

[redacted]

2011 Recommendation 5:
We recommend that APWUHP implement the necessary technical controls to its claims processing system to ensure that [redacted]

7. Explanation of Benefits

APWU's explanation of benefits (EOB) presentation for OBRA90 claims that include payments from other sources, such as Medicare Part B, could be confusing for subscribers.

a. 2007 Recommendation 44
We recommend that APWUHP revise its procedures so that non-covered benefits are not included on an OBRA90 claim in which the patient has Medicare Part B. Alternatively, APWUHP could use a remark code to state that the patient is not responsible for the non-covered benefit.

2007 APWU Response:
"The Health Plan will implement the alternative recommendation and use the remark code "Patient not responsible for amount over DRG pricing"."

2011 Status:
The OIG has confirmed that the recommended system modifications have been implemented; this recommendation is closed.

8. Special Investigations Unit

APWU was not in full compliance with Carrier Letter 2003-23 "Industry Standards for Fraud & Abuse (F&A) Programs" as required by OPM. We did not find evidence of an anti-fraud Policy statement, fraud hotlines for internal and external use, or fraud awareness educational material for enrollees.

a. 2007 Recommendation 45
We recommend that APWUHP implement all components of a comprehensive fraud and abuse program as required by carrier letter 2003-23.

2007 APWU Response:
"The Health Plan has reviewed the Carrier Letter 2003-23 and agrees some of the elements of the carrier letter need to be enhanced and reiterated with the employees of the Health Plan. Written policies/procedures will be updated and published to all employees. Training curriculums will be revised to ensure employees have an understanding of how to identify fraudulent claims."

2011 Status:
A separate OIG audit determined that all components of a comprehensive fraud and abuse program as required by carrier letter 2003-23 are not currently implemented at APWU. As a result of this audit, this recommendation remains open.

2011 Recommendation 6:
We recommend that APWU implement all components of a comprehensive fraud and abuse program as required by carrier letter 2003-23.

9. Sanctions Implementation Plan

APWU was not in full compliance with the "Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders," as required by the OPM OIG. Specifically, APWU's Sanction Implementation Plan does not address suspension processes and procedures, or approving regulatory authority for appeals.

a. 2007 Recommendation 46
We recommend that APWUHP update its Sanctions Implementation Plan to meet all the requirements set forth by OPM. These requirements can be found on OPM's Debarment website under "Guidelines for Implementation of Federal Employees Health Benefits Program Debarment and Suspension Orders."

2007 APWU Response:

"The Health Plan has given approval to [redacted] *to enhance the* [redacted] *system in order to improve our Debarment procedures. Enhancement 6.68 is attached for your review."*

2011 Status:

The OIG has confirmed that the recommended updates to the Sanction Implementation Plan regarding OPM's debarment and suspension have been implemented; this recommendation is closed.

cc: John O'Brien
Director, Healthcare and Insurance

Shirley Patterson
Assistant Director for Federal Employee Insurance Operations