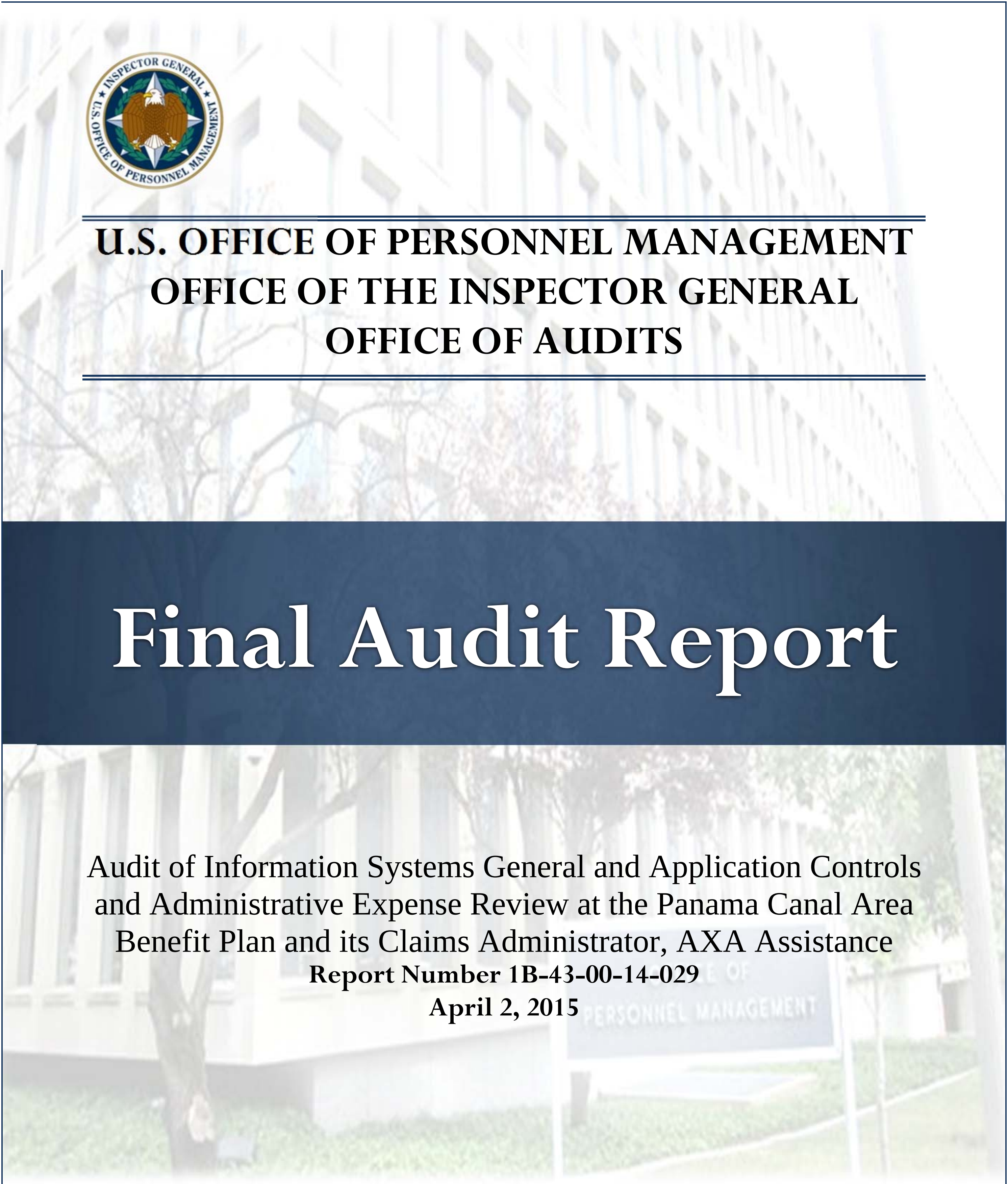

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Audit of Information Systems General and Application Controls and Administrative Expense Review at the Panama Canal Area Benefit Plan and its Claims Administrator, AXA Assistance

Report Number 1B-43-00-14-029

April 2, 2015

-- CAUTION --

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

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls and Administrative Expenses at the Panama Canal Area Benefit Plan and its claims administrator, AXA Assistance

Report No 1B-43-00-14-029 **April 2, 2015**

Background

The Panama Canal Area Benefit Plan (PCABP) contracts with the U.S. Office of Personnel Management (OPM) as part of the Federal Employees Health Benefits Program (FEHBP). PCABP subcontracts with a third-party claims administrator, AXA Assistance (AXA), to perform the vast majority of the work for OPM.

Why Did We Conduct the Audit?

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in AXA's information technology environment. We also analyzed administrative expenses to determine whether expenses charged to the contract were actual, allowable, necessary and reasonable expenses incurred in accordance with the terms of the contract and applicable regulations.

What Did We Audit?

The scope of this audit centered on the information systems used by AXA to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit at AXA determined that:

- AXA has established an adequate security management program.
- AXA has implemented controls to prevent unauthorized physical access to its facilities. However, we noted several areas of concern related to AXA's logical access controls:
  - There is no documented process to ensure proper segregation of duties within the claims adjudication application.
  - The password settings for user workstations are not in compliance with approved corporate standards.
- We noted several areas of concern related to AXA's network security controls:
  - A full scope vulnerability management program has not been implemented.
  - A patch management policy is in place, but our test work indicated that patches are not being implemented in a timely manner.
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized.
- AXA has not developed formal configuration policies/baselines for all databases used in its environment. Furthermore, AXA does not audit its database configuration against documented baseline configurations.
- AXA's business continuity and disaster recovery plans contain the key elements suggested by relevant guidance and publications. However, we noted several areas of concern related to AXA's contingency planning controls. AXA:
  - has not conducted a formal business impact analysis.
  - does not currently have an alternate recovery location.
  - does not conduct adequate contingency plan testing.
- AXA has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted a couple of weaknesses in AXA's claims application controls.
- AXA is in compliance with the Health Insurance Portability and Accountability Act security and privacy regulations.
- Administrative expenses charged to the FEHBP were actual, allowable, necessary, and reasonable expenses incurred in accordance with contract CS 1066 and applicable laws and regulations.

ABBREVIATIONS

AXA	AXA Assistance
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information System Controls Audit Manual
GAO	U.S. Government Accountability Office
HIO	Health Insurance Office
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
[redacted]	[redacted]
NIST	National Institute for Standards and Technology
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
PCABP	Panama Canal Area Benefit Plan
SP	Special Publication
The Act	Federal Employees Health Benefits Act

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) claims by the Panama Canal Area Benefit Plan (PCABP). PCABP subcontracts with a third-party claims administrator, AXA Assistance (AXA), to perform the vast majority of the work for its FEHBP contract.

The audit was conducted pursuant to FEHBP contract CS 1066; 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 (the 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 second audit of AXA's application controls and the first audit of general controls and administrative expenses. The first audit was conducted in 2008 and all recommendations from that audit were closed prior to the start of the current audit. We also reviewed AXA's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All AXA and PCABP 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 AXA's IT environment. We also evaluated whether administrative expenses charged to the contract were actual, allowable, necessary, and reasonable expenses incurred in accordance with the terms of the contract and applicable regulations. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to AXA's claims processing system;
- HIPAA compliance; and
- Administrative expenses.

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 AXA's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. We obtained an understanding of the internal controls over the cost accounting systems by inquiry of AXA officials. This understanding of AXA'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 AXA to process medical insurance claims for FEHBP members on behalf of the PCABP, with a primary focus on the claims adjudication applications. AXA claims are processed through a claims adjudication system called [redacted] ([redacted]). AXA licenses the [redacted] application from an external vendor. The business process reviewed is primarily located in AXA's Panama City, Panama location.

For the administrative expense review, we looked at AXA's FEHBP Annual Accounting Statements for contract years 2011, 2012 and 2013. We judgmentally reviewed administrative expenses charged to the FEHBP. Specifically, we reviewed administrative expenses relating to cost centers, natural accounts, out-of-system adjustments, and prior period adjustments. We used the FEHBP contract, the FAR, and the FEHBAR to determine the allowability, allocability, and reasonableness of charges.

The on-site portion of this audit was performed between June and August of 2014. 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 AXA as of August 2014.

In conducting our audit, we relied to varying degrees on computer-generated data provided by AXA. 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 audit we:

- Gathered documentation and conducted interviews;
- Reviewed AXA's business structure and environment;
- Performed a risk assessment of AXA'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 AXA's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the CFR;
- 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 FISCAM;
- 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 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- 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.

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATION

A. Security Management

The security management component of this audit involved the examination of the policies and procedures that are the foundation of AXA's overall IT security controls. We evaluated AXA's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

AXA maintains a series of thorough IT security policies and procedures.

AXA maintains a series of through IT policies and procedures that comprise its security management program. Nothing came to our attention to indicate that AXA does not have an adequate security management program.

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 AXA's facilities in Panama City, Panama and Chicago, Illinois and its data center in [redacted] Illinois. We also examined the logical controls protecting sensitive data on AXA's network environment and claims processing related applications.

The access controls observed during this audit include, but are not limited to:

- Procedures for granting and revoking logical access to information systems;
- Procedures for routinely auditing access to information systems; and
- Physical controls over facility and data center access.

The following sections document opportunities for improvement related to AXA's access controls.

1. Segregation of Duties

AXA does not have a documented process to ensure proper segregation of duties within its [redacted] claims adjudication application.

AXA restricts users' access rights within [redacted] using predefined roles. Rights are provisioned using a mirroring process in which one user's access rights are copied from an existing user's rights. However, there is no documented policy or procedure to indicate which roles would create an inherent conflict (i.e., too much control over the claims adjudication process) if granted to the same individual.

FISCAM states that "Work responsibilities should be segregated so that one individual does not control all critical stages of a process." FISCAM also states that "Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions."

Failure to enforce adequate segregation of duties in the claims processing application increases the risk that erroneous or fraudulent claims could be processed.

Recommendation 1

We recommend that the PCABP require AXA to implement a process for ensuring [redacted] application access is granted with proper segregation of duties.

PCABP Response:

"To improve the user's access process in [redacted] application, we are eliminating the mirroring process in which one user's access rights are copied from an existing user. We have modified the Access Form and created a [redacted] Access guide that includes the existing [redacted] Access & Role Chart for the IT department to ensure that proper rights are granted to new users account based on their role."

OIG Reply:

As part of the audit resolution process, we recommend that the PCABP provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this report that the PCABP and AXA agree to implement.

2. **Password Settings**

AXA's Privacy and Information Security Handbook outlines approved password composition settings. We reviewed the policy settings to determine if they conformed to industry best practices. We also compared the approved settings to the actual settings of AXA servers and workstations hosted in the Panama facility. While the approved settings conformed to industry best practice, AXA's password settings for user workstations in the Panama office are not in compliance with its own corporate standards.

Failure to configure password security settings in compliance with approved settings increases the risk that unauthorized users could gain access to sensitive resources.

Recommendation 2

We recommend that the PCABP require AXA to modify the password settings of the user workstations in Panama to comply with the AXA corporate password policy.

PCABP Response:

"AXA Panama has two domains. One domain is an old version which has not been discontinued since migration to the newer domain is not complete. All workstations and users in Panama are in the new domain. Nevertheless, we have configured the password settings of the older domain to be consistent to the new domain until it's discontinued."

OIG Reply:

As part of the audit resolution process, we recommend that the PCABP provide OPM's HIO with evidence that all user workstations in Panama are in the new domain, and that the password settings of that domain comply with the AXA corporate password policy.

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 AXA's network security program and performed several automated vulnerability scans during this audit. We noted the following opportunities for improvement related to AXA's network security controls.

1. Full Scope Vulnerability Scanning

We conducted a review of AXA's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities.

AXA does not conduct routine vulnerability scans on the entire network environment supporting the PCABP. Currently, scans are performed on a monthly basis for a limited subset of the network environment. Scan results are reviewed by AXA and necessary remediation is conducted on all network devices. However, this limited scope scanning process does not ensure weaknesses on all hosts are identified and remediated in a timely manner.

Failure to perform full scope vulnerability scanning increases the risk that AXA's systems could be breached and sensitive data could be stolen or destroyed.

NIST SP 800-53 Revision 4 states that the organization should scan "for vulnerabilities in the information system and hosted applications . . . ."

Failure to perform full scope vulnerability scanning increases the risk that AXA's systems could be compromised and sensitive data stolen or destroyed.

<u>Recommendation 3</u>

We recommend that the PCABP require AXA to implement a process to routinely conduct vulnerability scanning on the entire network environment and remediate vulnerabilities detected during scans in a timely manner.

<u>PCABP Response:</u>

"Our IT Security Manager will conduct vulnerability scanning [redacted] to identify any patches or updates needed so that local IT can patch or update any vulnerabilities.

The local IT team will work with the IT Security manager to ensure all vulnerabilities are addressed. Vulnerability scanning and patching for shared systems will be performed centrally for all regional systems.

By the end of Q1 2015, AXA Assistance USA will also implement tools, such as [redacted], which will help implement the patches and mitigate the manual work.

By the end of Q1 2015, the local IT team will setup a schedule and monitor that the maintenance schedule is followed."

2. Vulnerabilities Identified in Scans

System Patching

AXA has documented patch management policies and procedures. However, the results of our vulnerability scans indicate that all critical patches, service packs, and hot fixes are not implemented in a timely manner.

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 (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously.

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

<u>Recommendation 4</u>

We recommend that the PCABP require AXA to implement procedures and controls to ensure that production servers are kept up-to-date with appropriate patches, service packs, and hotfixes on a timely basis.

PCABP Response:

See response to recommendation three above. PCABP provided a single response for recommendations three, four and five.

Noncurrent software

Our vulnerability scans also indicated that several servers contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

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

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

Recommendation 5

We recommend that the PCABP require AXA to implement a process to ensure that only current and supported versions of software applications are installed on the production servers supporting the PCABP.

PCABP Response:

See response to recommendation three above. One response was provided for recommendations three, four and five.

D. Configuration Management

We evaluated AXA's management of the configuration of the operating systems and databases supporting [redacted] and determined that the following controls were in place:

- Documented corporate configuration policy, and
- Thorough change management procedures for system software and hardware.

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

1. Database Baseline Configuration

AXA has not documented a formal baseline configuration for its databases (note – the name of the specific database product has been redacted from this report). A baseline configuration is a formally approved standard outlining how to securely configure various operating platforms.

AXA has not documented baseline configurations for its databases.

NIST SP 800-53 Revision 4 states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not meet performance requirements defined by the organization.

Recommendation 6

We recommend that the PCABP require AXA to document approved baseline configurations for its databases.

PCABP Response:

"Documentation for a baseline [database] configuration has been acquired. AXA Assistance USA will determine a plan of action to implement and formalize a baseline for [database] configuration."

2. Configuration Compliance Auditing

As noted above, AXA does not maintain approved operating platform security configurations for its databases, and therefore cannot effectively audit the system's security settings (i.e., there are no approved settings to which to compare the actual settings).

As a result, AXA is also unable to conduct routine audits on the devices for compliance with the approved configuration settings.

NIST SP 800-53 Revision 4 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires "Current configuration information to be routinely monitored for accuracy. Monitoring should address the current baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 7

We recommend that the PCABP require AXA to implement a process to routinely audit its databases' security configuration settings to ensure they are in compliance with the approved configuration baseline.

PCABP Response:

"The baseline will be used to establish and formalize a periodic audit plan. The audit plan is expected to be implemented by the end of Q1 2015. The implementation activities will include setting up routine audits automatically through the tools used."

E. Contingency Planning

We reviewed AXA's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur. We determined that AXA has identified critical applications and that its service continuity documentation contained the critical elements suggested by NIST SP 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems." However, we found several areas for improvement related to AXA's contingency planning program.

1. Business Impact Analysis

AXA has not conducted a formal business impact analysis (BIA). During the fieldwork phase of the audit we were provided with a BIA template, but a formal process for conducting the BIA has not been fully implemented. All prior analysis related to identifying and prioritizing critical processes and applications was performed by informal discussions of high risk scenarios by AXA management.

NIST 800-34 Revision 1 states that a BIA is a key step in implementing the contingency planning process. Three steps involved in accomplishing a BIA include determining business processes and recovery criticality, identifying resource requirements, and identifying recovery priorities for system resources. Failure to conduct a BIA increases the risk that the organization will not be able to recover critical business operations in a timely manner.

Recommendation 8

We recommend that the PCABP require AXA to conduct a business impact analysis in accordance with NIST 800-34 Revision 1.

PCABP Response:

"A business impact analysis for all AXA Assistance USA operation is being prepared. A senior manager has been assigned to prepare an impact analysis and Business Continuity Plan (BCP) for all AXA Assistance USA operations. Information is being compiled by the local Panama office to prepare the impact analysis for the Panama Plan by Q1 of 2015. This information will be consolidated with the impact analysis for the Chicago and Miami locations to ensure a comprehensive BCP for the Panama Plan."

2. Alternate Recovery Location

AXA does not have an alternate location to recover its computing environment supporting the PCABP in the event of a disaster. Data is currently being replicated to a storage device in the same data center as the primary storage device. We were told that AXA is in the process of acquiring a backup location in [redacted] Missouri; however; the facility is not yet operational.

NIST SP 800-53 Revision 4 states that an organization must establish "an alternate processing site including necessary agreements to permit … the resumption of […information system operations] for essential missions/business functions . . . ." Failure to establish an alternate processing site prohibits AXA from continuing business operations in the event of a disaster at the primary data center.

<u>Recommendation 9</u>

We recommend that the PCABP require AXA to back up data and applications at an offsite location that is geographically separated from the primary site.

<u>PCABP Response:</u>

"The back-up center in [redacted] has been obtained and is being built out. Data from [redacted] supporting the Panama Plan is being backed up. The team will continue to build out Business Continuity Plan support capabilities including preparing redundant copies of core applications e.g. [redacted]."

3. Contingency Plan Testing

AXA does not perform adequate contingency plan testing. AXA routinely performs recovery exercises to verify that test data can be restored. However, the exercises do not involve restoration of software applications.

AXA's contingency plans are not adequately tested.

NIST SP 800-34 Revision 1 states that contingency plan testing "is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan." Failure to restore critical applications as part of the contingency plan testing increases the risk that AXA will not be able to continue business operations if unexpected events occur.

<u>Recommendation 10</u>

We recommend that the PCABP require AXA to conduct full contingency plan testing to ensure critical business applications and processes can be restored at an alternate recovery location.

<u>PCABP Response:</u>

"Testing of critical business applications will be performed during BCP testing which is scheduled to be completed by June 30, 2015."

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting AXA's claims adjudication process. The following recommendations are all addressed toward AXA's claims system supporting the PCABP, [redacted].

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of AXA's claims processing systems.

AXA has implemented policies and procedures related to application configuration management, and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- AXA has adopted practices that allow modifications to be tracked throughout the change process; and
- AXA uses a business unit independent from the software developers to move the code between development and production environments to ensure adequate segregation of duties.

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

2. Claims Processing System

We evaluated the input, processing, and output controls associated with AXA's claims processing system. We determined that AXA has implemented policies and procedures to help ensure that:

- Paper claims that are received in the member service area are tracked to ensure timely scanning and processing;
- Claims are reviewed as they are processed through the system; and
- Claims scheduled for payment are actually paid.

3. Enrollment

We evaluated AXA's procedures for managing its database of member enrollment data. Changes to member enrollment information are received electronically or in paper format, and enrollment information is manually entered into the claims processing system. Every enrollment transaction is audited to ensure information is entered accurately. We do not have any concerns regarding AXA's enrollment policies and procedures.

4. Debarment

AXA has adequate procedures for updating its claims system with debarred provider information. AXA downloads the OPM OIG debarment list every month and enters the information into its claims processing system. Any debarred providers that appear in AXA's provider database are flagged to prevent claims submitted by that provider from being processed successfully during the claims adjudication process.

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

5. Application Controls Testing

We conducted a test of AXA's claims adjudication application to validate the system's claims processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which AXA's claims processing system, [redacted], processed and adjudicated the claims.

Our test results indicate that the system has controls and edits in place to identify the following scenarios:

- Member eligibility;
- Exact duplicates;
- Gender/Procedure inconsistency;
- Procedure/Provider inconsistency;
- Coordination of benefits with worker's compensation;
- Bundling charges;
- Timely filing;
- Chiropractic benefits;
- Invalid place of service; and
- Once in a lifetime procedures.

The sections below document opportunities for improvement related to AXA's claims application controls.

a. Medical Editing

Our claims testing exercise identified scenarios where the claims processing system failed to detect medical inconsistencies. For the following scenarios, a test claim was processed and paid without encountering any edits detecting the [redacted] inconsistency:

- [redacted]
- [redacted]

Failure to detect this system weakness increases the risk that benefits are being paid for procedures that were not actually performed.

Recommendation 11

We recommend that the PCABP require AXA to make the appropriate system modifications to prevent medically inconsistent claims from processing.

PCABP Response:

"Our claims management system has [redacted] limits set up for the benefits limitation structure specific to the Plan Brochure. Although the plan has not paid any [redacted], we added the system [redacted] limits controls to the following benefits:

1. [redacted]
2. [redacted]

The system will deny [redacted] to [redacted]."

b. Benefit Structure

Our claims testing exercise identified scenarios where AXA's claims system failed to detect benefit structure issues. For the following scenario, a test claim was processed and paid without encountering any edits:

- [redacted]

Recommendation 12

We recommend that the PCABP require AXA to ensure the appropriate system modifications are made to prevent claims with benefit structure inconsistencies from processing.

PCABP Response:

"[redacted] is a procedure that requires a preauthorization. [redacted] frequency is controlled through our preauthorization process by the Medical Department. The Medical team then reviews for frequency and medical necessity. Nevertheless, we have included [redacted] frequency as new criteria through our weekly error detection report review as an additional control to ensure it's being paid accordingly, or authorized by the Medical Team in a lower frequency as medically necessary."

G. Health Insurance Portability and Accountability Act

We reviewed AXA's efforts to maintain compliance with the security and privacy standards of HIPAA.

AXA Assistance has implemented a collection of IT security policies and procedures to address the requirements of the HIPAA security rule. AXA has also developed a series of privacy policies and procedures that address requirements of the HIPAA privacy rule. AXA reviews its HIPAA privacy and security policies annually and updates when necessary. AXA's compliance office oversees all HIPAA activities, and helps develop, publish, and maintain corporate policies. Privacy and security training is provided periodically to all employees.

Nothing came to our attention to indicate that AXA is not in compliance with the various requirements of HIPAA regulations.

H. Administrative Expenses

We reviewed administrative expenses relating to cost centers, natural accounts, out-of-system adjustments, and prior period adjustments for contract years 2011, 2012, and 2013. We did not detect any findings pertaining to administrative expenses. Overall, we concluded that administrative expenses charged to the FEHBP were actual, allowable, necessary, and reasonable expenses incurred in accordance with Contract CS 1066 and applicable laws and regulations.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], Lead Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

Appendix

January 6, 2015

[redacted]
United States Office of Personnel Management
Office of the Inspector General
Information Systems Audits Group
Washington, DC 20415-1100

Re: Draft Report Response for the Application Controls Audit
Report No. 1B-43-00-14-029
Carrier Code: 43

Dear [redacted]:

On November 6, 2014 the U.S. Office of Personnel Management, Office of the Inspector General, Information Systems Audits Group issued a draft report for the Application Controls and Administrative Expense Review Audit of the Panama Canal Area Benefit Plan and administrator, AXA Assistance.

Our comments below are in response to the draft report detailing the results of the audit findings and recommendations of the Federal Employees Health Benefits Program operations.

Thank you for your cooperation and consideration of this additional information. If you have any questions or need additional information please contact me.

Sincerely,

Roberto Serbinio, President
The Association of Retirees of the Panama Canal Area

cc: [redacted]

ACCESS CONTROL

1. Segregation of Duties Recommendation

The Information Systems Audits Group recommended that AXA Assistance implement a process for ensuring [redacted] application access is granted with proper segregation of duties.

> To improve the user's access process in [redacted] application, we are eliminating the mirroring process in which one user's access rights are copied from an existing user. We have modified the Access Form and created a [redacted] Access guide that includes the existing [redacted] Access & Role Chart for the IT department to ensure that proper rights are granted to new users account based on their role.
>
> **Access Form:** This Form is used for any user access requests and must be completed by a department manager or supervisor. We have removed the User to Model After section to prevent a mirroring process in which one user access right are copied from an existing user rights. The department manager or supervisor will be required to indicate the title of the employee. *If new user has a title not listed in the [redacted] Access & Roles Chart, IT will work with the Manager in predefining access and update the role chart accordingly.*
>
> [redacted] **Access Guide:** This document was created as a formal guide on how to fill the information when creating a new [redacted] user account based on Title and Department.
>
> [redacted] **Access and Roles Chart:** This document has all the necessary information to create a new [redacted] user account by position and department

2. Password Settings Recommendation

The Information Systems Audits Group recommended that AXA Assistance modify the password settings of the user workstations in Panama to comply with its corporate policy.

> AXA Panama has two domains. One domain is an old version which has not been discontinued since migration to the newer domain is not complete. All workstations and users in Panama are in the new domain. Nevertheless, we have configured the password settings of the older domain to be consistent to the new domain until it's discontinued.

NETWORK SECURITY

3. Full Scope Vulnerability Scanning Recommendation

The Information Systems Audits Group recommended the following:

- ***AXA Assistance implement a process to routinely conduct vulnerability scanning on the entire network environment and remediate vulnerabilities detected during scans in a timely manner.***

- ***The Information Systems Audits Group recommended that AXA Assistance implement procedures and controls to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.***

- ***The Information Systems Audits Group also recommended that AXA Assistance implement a process to ensure that only current and supported versions of software applications are installed on the production servers.***

Our IT Security Manager will conduct vulnerability scanning [redacted] to identify any patches or updates needed so that local IT can patch or update any vulnerabilities.

The local IT team will work with the IT Security manager to ensure all vulnerabilities are addressed. Vulnerability scanning and patching for shared systems will be performed centrally for all regional systems.

By the end of Q1 2015, AXA Assistance USA will also implement tools, such as [redacted], which will help implement the patches and mitigate the manual work.

By the end of Q1 2015, the local IT team will setup a schedule and monitor that the maintenance schedule is followed.

CONFIGURATION MANAGEMENT

4. <u>[Database] Baseline Configuration Recommendation</u>

The Information Systems Audits Group recommended that AXA Assistance document approved baseline configurations for [its] databases.

Documentation for a baseline [database] configuration has been acquired. AXA Assistance USA will determine a plan of action to implement and formalize a baseline for [redacted] configuration.

5. <u>Configuration Compliance Auditing Recommendation</u>

The Information Systems Audits Group recommended that AXA Assistance implement a process to routinely audit [its] databases' security configurations settings to ensure they are in compliance with the approved configuration baseline.

The baseline will be used to establish and formalize a periodic audit plan. The audit plan is expected to be implemented by the end of Q1 2015. The implementation activities will include setting up routine audits automatically through the tools used.

CONTIGENCY PLANNING

6. *Business Impact Analysis Recommendation*

The Information Systems Audits Group recommended that AXA Assistance conduct a business impact analysis in accordance with NIST 800-34 Revision 1.

A business impact analysis for all AXA Assistance USA operation is being prepared. A senior manager has been assigned to prepare an impact analysis and Business Continuity Plan (BCP) for all AXA Assistance USA operations. Information is being compiled by the local Panama office to prepare the impact analysis for the Panama Plan by Q1 of 2015. This information will be consolidated with the impact analysis for the Chicago and Miami locations to ensure a comprehensive BCP for the Panama Plan.

7. *Alternate Recovery Location Recommendation*

The Information Systems Audits Group recommended that AXA Assistance back up data and applications at an offsite location that is geographically separated from the primary site.

The back-up center in [redacted] has been obtained and is being built out. Data from [redacted] supporting the Panama Plan is being backed up. The team will continue to build out Business Continuity Plan support capabilities including preparing redundant copies of core applications e.g. [redacted].

8. *Contingency Plan Testing Recommendation*

The Information Systems Audits Group recommended that AXA Assistance conduct full contingency plans testing to ensure critical business applications and processes can be restored at an alternate recovery location.

Testing of critical business applications will be performed during BCP testing which is scheduled to be completed by June 30, 2015.

CLAIM ADJUDICATION

9. Application Controls Testing Recommendation

a. Medical Editing

- **The Information Systems Audits Group recommended that AXA Assistance make the appropriate system modifications to prevent medically inconsistent claims from processing.**

Our claims management system has [redacted] limits set up for the benefits limitation structure specific to the Plan Brochure. Although the plan has not paid [redacted], we added the system [redacted] limits controls to the following benefits:

1. [redacted]

2. [redacted]

The system will deny [redacted] to [redacted].

b. ***Benefit Structure***

- **The Information Systems Audits Group recommended that AXA Assistance ensure the appropriate system modifications are made to prevent claims with benefit structure inconsistencies from processing.**

[redacted] is a procedure that requires a preauthorization. [redacted] frequency is controlled through our preauthorization process by the Medical Department. The Medical team then reviews for frequency and medical necessity. Nevertheless, we have included [redacted] frequency as new criteria through our weekly error detection report review as an additional control to ensure it's being paid accordingly, or authorized by the Medical Team in a lower frequency as medically necessary.

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

-- CAUTION --

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