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 at AultCare Health Plan

Report Number 1C-3A-00-15-012
January 21, 2016

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at AultCare Health Plan

Report No. 1C-3A-00-15-012 **January 21, 2016**

Why Did We Conduct the Audit?

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of Federal Employee Health Benefit Plan (FEHBP) data processed and maintained in the AultCare Health Plan (AultCare) information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by AultCare 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 of the IT security controls of AultCare determined that:

- AultCare has established an adequate security management program.
- AultCare has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, there is no technical control to detect or prevent [redacted] at AultCare's data center and other sensitive areas at its facility.
- AultCare has implemented an incident response and network security program. However, we noted several areas of concern related to AultCare's network security controls:
  - AultCare has not determined what auditable events should be logged and reviewed as a part of its incident response program.
  - A firewall baseline configuration standard is not in place.
  - [redacted]
  - [redacted]
  - AultCare's vulnerability management program could be improved.
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized.
- AultCare has developed a configuration management process for its operating platforms. However, formal baseline configuration standards are not in place for all servers and database platforms used by AultCare, and routine compliance auditing is not conducted.
- AultCare has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
AultCare	**AultCare Health Plan**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Plan**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OIG	**Office of the Inspector General**
OMB	**Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
SP	**Special Publication**

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 AultCare Health Plan (AultCare).

The audit was conducted pursuant to FEHBP contract CS 2723; 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.

All AultCare 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.

This was our first audit of AultCare's information technology (IT) general and application controls. We discussed the results of our audit with OPM and AultCare representatives at an exit conference.

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 AultCare's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to AultCare's claims processing systems.

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 AultCare's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of AultCare'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 AultCare to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. The business processes reviewed are primarily located in AultCare's Canton, Ohio facility.

The on-site portion of this audit was performed in February and March of 2015. 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 AultCare as of April 2015.

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

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed AultCare's business structure and environment;

- Performed a risk assessment of AultCare's information systems environment and applications, and prepared an audit program based on the assessment and the 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 AultCare's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- 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 (NIST) Special Publication (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 Information Technology Systems;
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide.

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

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

AultCare has implemented a series of formal policies and procedures that comprise its security management program. AultCare has also developed a thorough risk management methodology that allows AultCare to document, track, and mitigate or accept identified risks in a timely manner. AultCare also has adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Although it does have many security management controls in place, AultCare does not have a formal training requirement for individuals with specialized IT security responsibility.

AultCare has developed a thorough risk management methodology.

NIST SP 800-53, Revision 4, requires organizations to provide role-based security training to personnel with assigned security roles and responsibilities.

Requiring employees with specialized IT security responsibility to take routine training specifically tailored for their assigned duties increases their ability to address the constant changes in IT security best-practices.

Recommendation 1

We recommend that AultCare implement requirements for routine training for employees with specialized IT security responsibility.

AultCare Response:

"COMPLETE - AultCare agrees and has updated all applicable job descriptions with mandatory annual training hours."

OIG Reply:

In its response to our draft audit report AultCare provided sufficient evidence to address this recommendation; no further action is required.

B. Access Controls

Access controls are the policies, procedures, and controls used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls at AultCare's facilities and data centers located in [redacted] and [redacted], Ohio. We also examined the logical controls protecting sensitive data in AultCare's network environment and applications.

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

- Procedures for appropriately granting physical access to facilities and data centers;
- Procedures for appropriately granting, adjusting, and removing information system access;
- Strong environment controls within the data centers; and
- Controls to monitor and filter e-mail and Internet activity.

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

1) Access to the Primary Data Center, Sensitive Areas, and Data Center Co-Location

AultCare's office space is located within the Aultman Hospital facility, and electronic access cards are used to access the AultCare floors. AultCare's primary data center, staging room, and telecommunication room are located onsite within this office space, and are protected by an additional card reader. However, we expect the data center and other sensitive spaces of all FEHBP contractors to have the following additional controls:

- A technical or physical control to detect or prevent [redacted]; and
- [redacted].

AultCare's data center co-location (backup data center) does require [redacted], but it does not have [redacted] or [redacted].

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data. NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," provides guidance for adequately controlling physical access to information systems containing sensitive data.

Recommendation 2

We recommend that AultCare conduct a review of its physical access controls and implement some form of [redacted], [redacted], and [redacted] (co-location only) for the data centers and other sensitive areas at its facilities.

AultCare Response:

"IN PROCESS - AultCare is evaluating current physical access controls and actively quoting available options. An [redacted] policy is being created and AultCare will implement mandatory staff training by [redacted]. Implementation of [redacted] and [redacted] (co-location only) is projected to take place by [redacted]."

OIG Reply:

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

2) Physical Access Recertification

AultCare has implemented procedures to remove physical access privileges for terminated employees. However, AultCare does not have a process in place to periodically audit a list of individuals with physical access privileges against a list of current employees. In addition to ensuring that the access cards for terminated employees have been disabled, the audit should ensure that the level of access granted to each employee is appropriate and only allows them access to the areas necessary to perform their job function.

We independently compared a list of employees with active access to the AultCare facility to a list of employees that were terminated within the last year, and discovered that several employees retained access to the facility after their termination.

NIST SP 800-53, Revision 4, states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to audit physical access privileges increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information.

Recommendation 3

We recommend that AultCare implement a process for routinely auditing all active access cards to ensure that they are not assigned to terminated employees, and that the areas of access granted to each employee is appropriate to their position. This process should include written confirmation from managers.

AultCare Response:

"COMPLETE - AultCare agrees with this recommendation, established the baseline and implemented a policy as of May 2015. AultCare began performing weekly routine audits to monitor this activity in May 2015 and continues to do so."

OIG Reply:

In its response to our draft audit report AultCare provided sufficient evidence to address this recommendation; no further action is required.

C. Network Security

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

AultCare has implemented an incident response and network security program. However, we noted several opportunities for improvement related to AultCare's network security controls.

1) Audit Logging

AultCare has documented policies and procedures related to incident response. However, AultCare has not determined what auditable events its information systems can and should log, and has not implemented a process to routinely review system logs.

AultCare could improve its controls related to system logging and monitoring.

NIST SP 800-53, Revision 4, states that an organization must determine the information system is capable of auditing a list of defined events set by the organization. NIST also states that the organization should review and analyze the information system audit records and report the findings.

Failure to log and review information system auditable events increases the risk that AultCare will not be able to identify and respond to security incidents in a timely manner.

Recommendation 4

We recommend that AultCare determine what auditable events its information systems are capable of recording, determine which events are beneficial to log, and implement the technical changes to begin collecting log data. In addition, AultCare should implement a procedure for routinely reviewing the audit logs.

AultCare Response:

"IN PROCESS - AultCare agrees and has software in place including [redacted], [redacted] and, as of October 12, 2015, [redacted] that actively tracks network and system management logs. The logs are reviewed on a routine basis."

2) Firewall Management

AultCare has implemented firewalls to protect its network environment, and we did not identify any concerns with the firewall architecture. However, AultCare has not established a formal firewall baseline configuration standard, nor a procedure to routinely audit current firewall settings against a baseline.

NIST SP 800-41, Revision 1, states that a firewall policy should dictate how firewalls handle network traffic based on the organization's information security policies, and a risk analysis should be performed to determine types of traffic needed by the organization. The policy should also include specific guidance on how to address changes to the rule set.

Failure to develop a firewall configuration policy and manage the settings increases AultCare's exposure to unsecure traffic and vulnerabilities.

Recommendation 5

We recommend that AultCare develop a corporate firewall baseline configuration and implement a process for routinely auditing actual firewall settings against the baseline.

AultCare Response:

"IN PROCESS - AultCare agrees with the recommendation and has begun the process of establishing an independent firewall and creating the baseline. The estimated completion date for this project is [redacted]."

3) [redacted]

Recommendation 6

We recommend that AultCare implement [redacted].

AultCare Response:

"IN PROCESS - AultCare agrees and is in the process of [redacted]. Full implementation is expected by [redacted]."

4) [redacted]

Recommendation 7

[redacted]

AultCare Response:

"IN PROCESS - AultCare agrees and is beginning to establish [redacted] ***. Expected implementation date is*** [redacted] ***."***

5) Vulnerability Scanning/Remediation

AultCare should perform routine vulnerability scanning on its systems.

AultCare utilizes a 3rd party contractor to conduct annual penetration testing on its technical environment. After the testing has been completed, AultCare works to remediate any vulnerabilities identified in a timely manner. However, AultCare does not have its own vulnerability scanning tools nor procedures to conduct more routine scans and remediate any vulnerabilities identified. It is best practice to perform vulnerability scanning on a relatively frequent basis (measured in weeks or months, but not annually) - especially in today's IT security environment where new vulnerabilities are discovered on a daily basis.

NIST SP 800-53 states that an organization should routinely scan for vulnerabilities in the information systems and hosted applications. It also states that an organization should analyze vulnerability scan reports and results, then remediate the legitimate vulnerabilities.

Failure to identify and remediate known vulnerabilities greatly increases the organization's risk to easily exploited weaknesses. This may lead to a loss of personal health information and control of information systems and applications.

Recommendation 8

We recommend that AultCare implement a process to perform routine automated vulnerability scans to ensure all known weaknesses within the information systems are identified in a timely manner. This process should include a methodology to analyze the vulnerability scan reports, identify legitimate vulnerabilities, and remediate them in a timely manner and/or document the acceptance of the risk.

AultCare Response:

"IN PROCESS - AultCare agrees with this recommendation and contracted with [redacted], a third party, to complete a Vulnerability Scan in May 2015. Results are available upon request. Remediation of the results is in process. AultCare will continue to have third party scans performed annually, at a minimum."

OIG Reply:

Contracting vulnerability assessment work to a vendor is an acceptable approach to implementing this recommendation. However, as stated above, it is best practice to perform vulnerability scanning on a relatively frequent basis (measured in weeks or months, but not annually). Scanning only once per year increases the risks that unknown or un-remediated vulnerabilities exist for an extended period of time. We continue to recommend that AultCare perform weekly or monthly automated vulnerability scans in addition to its annual penetration test work.

6) Vulnerabilities Identified in Scans

OIG test work identified a variety of system vulnerabilities that could have been detected by a mature vulnerability assessment program.

As mentioned above, we believe that AultCare's vulnerability management program could be improved. As part of this audit, we also independently performed our own automated vulnerability scans on a sample of AultCare's servers, databases, web applications, and user workstations. Our test work identified a variety of vulnerabilities that could have potentially been previously detected and remediated by AultCare if it had a more mature vulnerability management program in place. The specific vulnerabilities that we identified will not be detailed in this report, but are summarized at a high level below. Copies of the full scan reports were provided directly to AultCare during the audit.

System Patching

AultCare appears to be generally compliant with its patch management policies and procedures. However, our scans detected several instances where critical patches were not installed in accordance with the policy. The missing patches included both operating system and third-party software.

Antivirus Updates
The results of the vulnerability scans indicated that several installations of AultCare's antivirus software tool had out of date antivirus signatures.

Noncurrent Software
The results of the vulnerability scans indicated that several servers and workstations contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities. AultCare had not documented a business need to maintain this software.

Server Configuration Vulnerabilities
The results of our scans identified that isolated server configuration vulnerabilities with known exploits exist in AultCare's technical environment.

Web Application Vulnerabilities
The results of the web application vulnerability scans also indicated that the AultCare web application has several vulnerabilities that are susceptible to common malicious attack methods.

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

The vulnerabilities identified in our test work increase the risk that a malicious attack on AultCare's technical environment would be successful.

Recommendation 9
We recommend that AultCare make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.

AultCare Response:
"IN PROCESS - AultCare agrees and has been addressing the results of the May 2015 external vulnerability scan. AultCare itself will be purchasing a scanning system, but will also continue to have a third party vendor scan annually. Results of each scan will be addressed accordingly. AultCare scanning system expected implementation date is June 30, 2016."

Recommendation 10

We recommend that AultCare implement a methodology to ensure that only current and supported versions of system software are installed on the production servers and workstations. If a business need necessitates the use of outdated software, AultCare should document this exception.

AultCare Response:

"IN PROCESS - AultCare agrees with this recommendation and is currently in the process of evaluating [redacted]. Expected implementation date is [redacted]."

D. Configuration Management

We evaluated AultCare's configuration management program as it relates to the operating platforms that support the processing of FEHBP claims, and determined that the following controls were in place:

- Established server build documents; and
- A system software change control process.

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

1) Security Baseline Configurations

AultCare has not documented security baseline configuration standards for all operating platforms used in its technical environment. A baseline configuration is a formally approved policy or standard outlining how to securely configure an operating platform.

NIST SP 800-53, Revision 4, states that an organization should 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 or security requirements defined by the organization.

Recommendation 11

We recommend that AultCare document approved baseline configurations for all server and database platforms used in its environment.

AultCare Response:

"IN PROCESS - AultCare agrees and is in the process of creating Configuration Policies to document approved baselines for both [redacted] and [redacted]. The policies will be complete by December 31, 2015."

2) Configuration Compliance Auditing

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

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

Failure to 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.

Recommendation 12

We recommend that AultCare routinely audit all server and database security configuration settings to ensure they are in compliance with approved baselines.

AultCare Response:

"IN PROCESS - AultCare agrees and is in the process of documenting the approved baseline configurations. Upon completion, AultCare will begin routine audits. Implementation is to be expected by July 31, 2016."

E. Contingency Planning

We reviewed the following elements of AultCare's contingency planning program to determine whether controls were in place to prevent or minimize interruptions to business operations when disrupting events occur:

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

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

AultCare has developed a thorough disaster recovery plan, but has not completed a feasibility assessment or a functional test of this plan.

The sections below document areas for improvement related to AultCare's contingency planning controls.

1) Feasibility Assessment

AultCare's current business continuity plan involves the use of approximately 20 user workstations that are stored at the backup facility. These machines would be loaded with the necessary software and provided to the users to continue AultCare's business operations. However, AultCare's employee population is approximately 500 individuals, and AultCare has not conducted a feasibility assessment to ensure that the number of on hand workstations would meet the needs of the organization in the event of a disaster.

NIST SP 800-53, Revision 4, states an organization should develop a contingency plan that identifies essential missions and business functions and the associated contingency requirements.

Failure to evaluate the feasibility of the business continuity plan increases the risk that an organization cannot maintain business operations when disrupting events occur.

Recommendation 13

We recommend that AultCare conduct a feasibility assessment on the current contingency plan to ensure that it can meet the objectives set by the organization in the event of a disruption.

AultCare Response:

"IN PROCESS - AultCare agrees with this recommendation and will conduct a contingency plan feasibility test during first quarter of 2016. The estimated date of completion is March 1, 2016."

2) Functional Disaster Recovery Tests

AultCare has documented disaster recovery plans and conducts routine disaster recovery tabletop tests. However, AultCare has not conducted a functional disaster recovery test. This is further compounded by the fact that AultCare has not conducted a feasibility assessment to ensure they have the proper resources in place to recover from a disrupting situation.

NIST SP 800-53, Revision 4, states that an organization should test the contingency plan for the information system to determine the effectiveness of the plan and organization readiness to execute the plan.

Functional disaster recovery tests allow an organization to evaluate the effectiveness of the contingency plan. Failure to do so increases the risk that an organization cannot recover from a disrupting situation in a timely manner.

Recommendation 14

We recommend that AultCare routinely conduct functional tests of its disaster recovery test to evaluate its effectiveness.

AultCare Response:

"COMPLETE - AultCare agrees and has completed a two part Functionality test which was concluded in October 2015."

OIG Reply:

In its response to our draft audit report AultCare provided sufficient evidence to address this recommendation; no further action is required.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting AultCare's claims adjudication process.

1) Application Change Management

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

AultCare has implemented a thorough application change management program.

AultCare 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:

- AultCare has adopted practices that allow modifications to be tracked throughout the change process;
- Code, unit, system, and quality testing are all conducted in accordance with industry standards; and
- AultCare 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 AultCare has not implemented adequate controls related to the application configuration management process.

2) Claims Input, Processing, and Output Controls

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

- Routine reviews are conducted on AultCare's front-end scanning process for incoming paper claims;
- Claims are monitored as they are processed through the system; and
- Claims output files are fully reconciled.

During the review of the physical environment for claims input we noted that checks are not secured after they are identified in incoming mail. Failure to protect financial assets increases the probability of loss.

Recommendation 15

We recommend that AultCare add a secure location for incoming checks in the mailroom.

AultCare Response:

"COMPLETE - AultCare agrees and created a Policy requiring all incoming FEHB[P] checks to be logged and housed in a locked cabinet until retrieved by the Finance."

OIG Reply:

In its response to our draft audit report AultCare provided sufficient evidence to address this recommendation; no further action is required.

3) Enrollment

We evaluated AultCare's procedures for managing its member enrollment data. Enrollment information is received electronically and compared to the member database. Necessary changes are reported to the eligibility office and updated in the database. Changes are verified during the next database comparison.

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

4) Debarment

We evaluated AultCare's procedures for updating its claims system with debarred provider information. AultCare downloads the OPM OIG debarment list every month and makes the appropriate updates to its claims processing system. Providers are flagged in the system for both future and past claims. Any claim submitted for a debarred provider is flagged by AultCare to adjudicate through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial of claims.

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

5) Special Investigation/Fraud

We evaluated AultCare's policies and procedures surrounding its efforts to detect fraud and abuse in the FEHBP line of business. AultCare has implemented a special investigations unit that has access to all employees and facilities for investigation purposes. AultCare's policy is to refer investigative cases to the OPM OIG only *after fraud is confirmed*. However, AultCare's contract with OPM requires AultCare to immediately notify our office of all *potential* fraud cases.

Recommendation 16

We recommend that AultCare update it policy to require the referral of all possible fraud cases to the OPM OIG.

AultCare Response:

"COMPLETE - AultCare agrees and updated the current Fraud Policy accordingly."

OIG Reply:

In its response to our draft audit report AultCare provided sufficient evidence to address this recommendation; no further action is required.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Lead IT Auditor-In-Charge
[redacted], Lead IT Auditor
[redacted], IT Auditor

[redacted], Group Chief

V. APPENDIX

November 16, 2015

AultCare Health Plan
[redacted], Compliance Officer
2600 6th St. SW
Canton, OH 44710

Reference: OPM Draft Audit Report
AultCare Health Plan IT Audit
Plan Code 3A
Audit Report Number 1C-3A-00-15-012

The following report represents AultCare Health Plan's response to the recommendations included in the Draft Audit Report dated September 16, 2015.

Security Management

Recommendation 1 - We recommend that AultCare implement requirements for routine training for employees with specialized IT security responsibility.

Response - COMPLETE - AultCare agrees and has updated all applicable job descriptions with mandatory annual training hours. See attachments A-1 – A-7.

Access Controls

Recommendation 2 - We recommend that AultCare conduct a review of its physical access controls and implement some form of [redacted], [redacted], and [redacted] (co-location only) for the data centers and other sensitive areas at its facility.

Response – IN PROCESS - AultCare is evaluating current physical access controls and actively quoting available options. An [redacted] policy is being created and AultCare will implement mandatory staff training by [redacted]. Implementation of [redacted] and [redacted] (co-location only) is projected to take place by [redacted].

Recommendation 3 - We recommend that AultCare implement a process for routinely auditing all active access cards to ensure that they are not assigned to terminated employees, and that the areas of access granted to each employee is appropriate to their position. This process should include written confirmation from managers.

Response - COMPLETE - AultCare agrees with this recommendation, established the baseline and implemented a policy as of May 2015. AultCare began performing weekly routine audits to monitor this activity in May 2015 and continues to do so. See attachments B-1 – B-2

Network Security

Recommendation 4 - We recommend that AultCare determine what auditable events its information systems are capable of recording, determine which events are beneficial to log, and implement the technical changes to begin collecting log data. In addition, AultCare should implement a procedure for routinely reviewing the audit logs.

Response – IN PROCESS - AultCare agrees and has software in place including [redacted], [redacted] and, as of October 12, 2015, [redacted] that actively tracks network and system management logs. The logs are reviewed on a routine basis.

Recommendation 5 - We recommend that AultCare develop a corporate firewall baseline configuration, and implement a process for routinely auditing actual firewall settings against the baseline.

Response – IN PROCESS - AultCare agrees with the recommendation and has begun the process of establishing an independent firewall and creating the baseline. The estimated completion date for this project is [redacted].

Recommendation 6 - We recommend that AultCare implement [redacted].

Response –IN PROCESS - AultCare agrees and is in the process of r[redacted]. Full implementation is expected by [redacted]

Recommendation 7 - [redacted].

Response – IN PROCESS - AultCare agrees and is beginning to establish an i[redacted]. Expected implementation date is [redacted].

Recommendation 8 - We recommend that AultCare implement a process to perform routine automated vulnerability scans to ensure all known weaknesses within the information systems are identified in a timely manner. This process should include a methodology to analyze the vulnerability scan reports, identify legitimate vulnerabilities, and remediate them in a timely manner and/or document the acceptance of the risk.

Response – IN PROCESS - AultCare agrees with this recommendation and contracted with [redacted], a third party, to complete a Vulnerability Scan in May 2015. Results are available upon request. Remediation of the results is in process. AultCare will continue to have third party scans performed annually, at a minimum.

Recommendation 9 - We recommend that AultCare make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.

Response – IN PROCESS - AultCare agrees and has been addressing the results of the May 2015 external vulnerability scan. AultCare itself will be purchasing a scanning system, but will also continue to have a third party vendor scan annually. Results of each scan will be addressed accordingly. AultCare scanning system expected implementation date is June 30, 2016.

Recommendation 10 - We recommend that AultCare implement a methodology to ensure that only current and supported versions of system software are installed on the production servers and workstations. If a business need necessitates the use of outdated software, AultCare should document this exception.

Response – IN PROCESS - AultCare agrees with this recommendation and is currently in the process of evaluating [redacted]. Expected implementation date is [redacted].

Configuration Management

Recommendation 11 - We recommend that AultCare document approved baseline configurations for all server and database platforms used in its environment.

Response – IN PROCESS - AultCare agrees and is in the process of creating Configuration Policies to document approved baselines for both [redacted] and [redacted]. The policies will be complete by December 31, 2015.

Recommendation 12 - We recommend that AultCare routinely audit all server and database security configuration settings to ensure that they are in compliance with approved baselines.

Response – IN PROCESS - AultCare agrees and is in the process of documenting the approved baseline configurations. Upon completion, AultCare will begin routine audits. Implementation is to be expected by July 31, 2016.

Contingency Planning

Recommendation 13 - We recommend AultCare conduct a feasibility assessment on the current contingency plan to ensure that it can meet the objectives set by the organization in the event of a disruption.

Response – IN PROCESS - AultCare agrees with this recommendation and will conduct a contingency plan feasibility test during first quarter of 2016. The estimated date of completion is March 1, 2016.

Recommendation 14 - We recommend AultCare routinely conduct functional tests of its disaster recovery to evaluate its effectiveness.

Response - COMPLETE - AultCare agrees and has completed a two part Functionality test which was concluded in October 2015. See attachments C-1 – C-2.

Claims Adjudication

Recommendation 15 - We recommend that AultCare add a secure location for incoming checks in the mailroom.

Response - COMPLETE - AultCare agrees and created a Policy requiring all incoming FEHB checks to be logged and housed in a locked cabinet until retrieved by the Finance. See attachments D-1 – D-2.

Recommendation 16 - We recommend that AultCare update its policy to require the referral of all possible fraud cases to the OPM OIG.

Response - COMPLETE - AultCare agrees and updated the current Fraud Policy accordingly. See attachment E.

Thank you for providing the opportunity to respond to your recommendations and provide an update for the Final Report. If you have any questions, please feel free to contact me at 330-363-1363.

Sincerely,

[redacted]
Compliance Officer
AultCare

Attachments A-E

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