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 DEAN HEALTH PLAN

Report Number 1C-WD-00-16-059
June 5, 2017

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Dean Health Plan

Report No. 1C-WD-00-16-059 **June 5, 2017**

Why Did We Conduct the Audit?

Dean Health Plan (DHP) contracts with the U.S. Office of Personnel Management to provide health insurance benefits for federal employees, annuitants, and qualified dependents as part of the Federal Employees Health Benefits Program (FEHBP).

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

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls at DHP determined that:

- DHP has established an adequate security management program.
- DHP has implemented both physical and logical access controls to prevent unauthorized access to its facilities and to sensitive information.
- DHP has implemented an incident response and network security program. However, DHP has not documented and approved a firewall configuration standard. Without a firewall configuration standard DHP cannot routinely review its firewalls for compliance against an approved baseline. DHP also has systems running software that is unsupported by the vendor, and DHP does not have a control in place to limit network access to authorized devices.
- DHP has developed configuration management policies and procedures. However, DHP has not documented and approved configuration standards for its systems. Without configuration standards DHP cannot routinely review its systems for compliance.
- DHP has established a risk-based contingency program with documented plans that identify critical systems and contain detailed recovery procedures. These plans and procedures are regularly reviewed and tested.
- DHP has implemented controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

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

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 Dean Health Plan (DHP or Plan).

The audit was conducted pursuant to FEHBP contract CS 1966; 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 DHP 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 DHP's information technology (IT) general and application controls. We discussed the results of our audit with OPM and DHP 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 DHP'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 DHP's claims processing systems.

SCOPE AND METHDOLOGY

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 DHP's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related policies and procedures. This understanding of DHP'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 DHP to process medical insurance claims and/or store data of FEHBP members, with a primary focus on the claims adjudication process. The business processes reviewed are primarily located in DHP's Madison, Wisconsin facility.

The on-site portion of this audit was performed in August and September of 2016. 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 DHP as of September 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by DHP. 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 DHP's business structure and environment;
- Performed a risk assessment of DHP'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 were 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 DHP's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether DHP's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, DHP 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

Security management encompasses the policies and procedures that are the basis of DHP's overall IT security program. We evaluated the DHP's ability to develop and maintain security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

DHP has developed formal IT security policies and procedures.

The Plan has implemented a series of formal policies and procedures that comprise its security management program. This includes an adequate risk management methodology and a process to create remediation plans addressing weaknesses identified in risk assessments. We also reviewed DHP's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that DHP 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 DHP's facilities and data centers. We also examined the logical controls protecting sensitive data on DHP's network environment and claims processing-related applications.

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

- Procedures for appropriately granting and removing physical access to facilities and data centers;
- Procedures for authorizing and revoking logical access to applications; and
- Routine access reviews.

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

1) Data Center Physical Access

The Plan's primary data center is located [redacted] and requires multi-factor authentication ([redacted]) to gain access. DHP has a back-up data center that is located in [redacted], and access to that area is controlled by [redacted]. The physical access controls of the back-up data center could be improved by requiring multi-factor authentication at all entrances (e.g., cipher lock or biometric device in addition to an access card). In addition, the physical access controls of both data centers could be improved with the implementation of piggybacking prevention or detection controls at all entrances (e.g., an alarm that sounds if more than one person walks past a sensor for each access card that is swiped).

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

Recommendation 1

We recommend that DHP implement multi-factor authentication at its back-up data center and implement piggybacking prevention or detection controls at both its primary and back-up data centers.

DHP Response:

"DHP agrees with the recommendation.

DHP has implemented the following to address this recommendation:
1. The back-up data center has installed multi-factor authentication ([redacted]) for data center access. The primary data center had multi-factor authentication installed prior to the audit.
2. A "piggybacking" solution has been installed at both the primary and back-up data centers that ties in to the security system. A piggybacking alarm is generated if anyone enters the data center without badging.

DHP believes this recommendation has been fully remediated."

OIG Comment:

Evidence was provided in response to the draft report that indicates that DHP has implemented the recommended controls; no further action is required.

C. NETWORK SECURITY

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

We evaluated DHP's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit. We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A thorough incident response program.

The following sections document several opportunities for improvement related to DHP's network security controls.

1) Documented Firewall Policy

DHP has firewalls strategically placed in locations throughout its network. However, the Plan has not formally documented a policy or standard that identifies the types of traffic allowed by the organization and the approved settings that are needed to harden firewalls within the network.

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

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

Recommendation 2

We recommend that DHP document and approve a firewall policy and/or configuration standard.

DHP Response:

"DHP agrees with the recommendation.

DHP is documenting a firewall policy and configuration standard that is customized to our technical environment. The expected completion date is the end of Q2 2017."

OIG Comment:

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

2) Firewall Configuration Review

DHP runs a daily firewall configuration report that indicates what, if any, rules have changed during that day. This control is valuable in helping the Plan detect unauthorized changes to the firewalls. However, as explained above, DHP is unable to adequately audit the current firewall configuration without an approved policy or standard for comparison. While our audit was in progress, DHP implemented a process to audit its firewalls' configuration using an automated scanning tool. The configuration settings are compared to generic benchmarks established by [redacted]. However, this process could be further improved by comparing the configuration to a firewall policy specific to DHP's technical environment and its associated risks.

NIST 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization's policies.

Failure to audit firewall configurations against the firewall policy or configuration standard increases the risk that the firewalls could be compromised and rules exist which allow unacceptable or unneeded network traffic.

Recommendation 3

We recommend that DHP perform routine audits of its current firewall configurations against an approved firewall policy that is customized to its technical environment. Note – this recommendation cannot be implemented until the controls from Recommendation 2 are in place.

DHP Response:

"DHP agrees with the recommendation.

Once the firewall policy is implemented (see #2), DHP will start periodic audits against the documented firewall configurations."

3) System Development Lifecycle

DHP leverages a variety of third-party software products in its technical environment. The vendors of these products typically publicize information related to the product's "end-of-life" support dates (dates when the vendor will no longer release security updates and patches). DHP stated that its efforts to decommission software begin 12 months before a known end-of-life date. However, our analysis of DHP's system inventory revealed multiple instances of servers running unsupported versions of operating systems. DHP has plans to remove these unsupported systems by the end of November 2016.

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

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

Recommendation 4

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

DHP Response:

"DHP agrees with the recommendation.

DHP will implement the following to address this recommendation:

1. ***DHP utilizes the [redacted] within [redacted] to maintain the inventory of applications. This inventory is used to track needed version upgrades and EOL. DHP will add Operating Systems and Databases to this tracking list so all can be tracked from one source. This will be completed by the end of Q1 2017.***
2. ***At the end of each annual budget cycle, IT management reviews the list from #1 above for all platforms, infrastructure, applications, and software that need to be upgraded in the next calendar year. This list is sorted from highest to lowest priority.***
3. ***IT management then submits a proposal to the Infrastructure Investment Review Board (IIRB) requesting funding for the items on the list.***
4. ***Once funding is approved, the funds are used to upgrade as many items as possible starting with the high priority items."***

4) Network Access Controls

DHP does not have controls to prevent non-company owned devices from connecting to its internal network. However, we were told that the Plan has purchased a network access control solution to address this problem, and aims to implement it by the end of 2017.

DHP is implementing a solution to prevent non-company owned devices from connecting to its network.

NIST 800-53, Revision 4, states that an information system should uniquely identify and authenticate devices before establishing a network connection.

Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

Recommendation 5

We recommend that DHP implement network access controls to prevent non-company owned devices from connecting to its internal network.

Plan Response:

"DHP agrees with the recommendation.

A security solution has been purchased. Implementation of a network access controls project will begin in early 2017 but due to the complexity of the scope a definite planned completion date cannot be determined at this time. As this project progresses DHP will be in a better position to narrow down a planned completion time."

D. CONFIGURATION MANAGEMENT

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

- Documented configuration management policy;
- Documented system change control process; and
- Adequate system patching process.

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

1) Security Configuration Standards

DHP has not documented formal security configuration standards for its computer servers or databases. A security configuration standard is a formally approved document that contains details on how security settings should be configured for specific operating platforms.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system . . . that reflect the most restrictive mode consistent with operational requirements . . . ." In addition, NIST SP 800-53, Revision 4, 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 systems may not be configured in a secure manner.

Recommendation 6

We recommend that DHP document approved security configuration settings for all operating platforms and databases deployed in its technical environment.

DHP Response:

"DHP agrees with the recommendation.

DHP will document all database and operating system security configuration standards by the end of Q3 2017."

2) Security Configuration Auditing

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

DHP cannot effectively audit its systems' security settings.

DHP has recently acquired an automated scanning tool that will allow it to conduct compliance audits of servers and databases within the network environment. Utilizing an automated compliance scanning tool to audit security settings against established security configuration standards will help ensure that servers and databases are appropriately hardened. However, DHP must have mature configuration standards in place (see Recommendation 6) before this tool can be fully effective.

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 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 7

We recommend that DHP implement a process to routinely audit the configuration settings of servers and databases to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

DHP Response:

"DHP agrees with this recommendation.

Once the database and operating system security configuration standards have been documented (see #6), DHP will implement processes to audit these settings to make sure they are in compliance with the approved standards."

E. CONTINGENCY PLANNING

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

- Disaster recovery plan and testing;
- Business continuity plan and testing; 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." DHP has identified and prioritized the systems and resources that are critical to business operations, and have developed detailed procedures to recover those systems and resources.

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

F. APPLICATION CONTROLS

The following sections detail our review of the applications and business processes supporting DHP's claims adjudication process. We reviewed the following processes related to the claims adjudication process: application configuration management, claims processing, member enrollment, and provider debarment.

1) Application Configuration Management

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

The Plan 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:

- Policies and procedures that allow modifications to be tracked throughout the change process;
- Unit, integration, and quality assurance testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

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

2) Claims Processing

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

- Documented policies and procedures for the input and processing of claims;
- Quality assurance reviews of claims processing; and

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

However, we noted one opportunity for improvement related to DHP's claims processing controls.

Paper Claims Tracking

During a walk-though of the claims processing workflow we noted that incoming paper claims are opened in one area, then transported to another building for sorting and batching, and then returned to the original location for scanning. DHP does not have a process in place to log or track paper claims as they are transported from one facility to another.

Failure to track paper claims increases the chances that claims could be lost or misplaced in transit which could lead to the unintended disclosure of sensitive information.

Recommendation 8

We recommend that DHP implement a process to verify that all paper claims are tracked throughout the claims adjudication process.

DHP Response:

"DHP agrees with the recommendation.

DHP has implemented the following to address the recommendation:

1. ***DHP now uses locked containers for transporting paper claims between buildings.***
2. ***Each container will have a log sheet showing*** [redacted] ***The same process is followed when claims are being returned to the mail room.***
3. ***Security for the mail room at*** [redacted] ***has been upgraded to require*** [redacted] ***for entry. Access to the mail room is limited to authorized staff only."***

OIG Comment:

DHP provided evidence in response to the draft report that the controls identified above had been implemented; no further action is required.

3) Enrollment

We assessed DHP's procedures for managing its member enrollment data. Enrollment information is received electronically or in paper format and is manually entered into the enrollment database. The Plan has resources dedicated to FEHBP enrollment and conducts quality reviews and audits to ensure that enrollment information is entered accurately and completely.

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

4) Debarment

DHP has documented procedures for reviewing provider files for debarments and suspensions. The Provider Services & Credentialing Department downloads the OPM OIG debarment list monthly and manually compares the list to the provider information system. Any matches are reviewed, discussed, and confirmed. If a match is found a hold is placed on the debarred provider in the claims processing system. Any claim submitted by a debarred provider is flagged to adjudicate through the OPM OIG debarment process. This process includes member notification, a 15-day grace period, and then denial of the claim.

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

APPENDIX

OPM Draft Audit Report Recommendation Comments

Dean Health Plan

1/25/2017

Recommendation 1 – Access Controls: Data Center Physical Access

We recommend that DHP implement multi-factor authentication at its back-up data center and implement piggybacking prevention or detection controls at both its primary and back-up data centers.

DHP Response:

DHP agrees with the recommendation.

DHP has implemented the following to address this recommendation:

1. *The back-up data center has installed multi-factor authentication ([redacted]) for data center access. The primary data center had multi-factor authentication installed prior to the audit.*
2. *A "piggybacking" solution has been installed at both the primary and back-up data centers that ties in to the security system. A piggybacking alarm is generated if anyone enters the data center without badging.*

DHP believes this recommendation has been fully remediated.

Recommendation 2 – Network Security: Documented Firewall Policy

We recommend that DHP document and approve a firewall policy and/or configuration standard.

DHP Response:

DHP agrees with the recommendation.

DHP is documenting a firewall policy and configuration standard that is customized to our technical environment. The expected completion date is the end of Q2 2017.

Recommendation 3 – Network Security: Firewall Configuration Review

We recommend that DHP perform routine audits of its current firewall configurations against an approved firewall policy that is customized to its technical environment. **Note** – this recommendation cannot be implemented until the controls from Recommendation 2 are in place.

DHP Response:

DHP agrees with the recommendation.

Once the firewall policy is implemented (see #2), DHP will start periodic audits against the documented firewall configurations.

Recommendation 4 – Network Security: System Development Lifecycle

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

DHP Response:

DHP agrees with the recommendation.

DHP will implement the following to address this recommendation:

1. *DHP utilizes the* [redacted] *within* [redacted] *to maintain the inventory of applications. This inventory is used to track needed version upgrades and EOL. DHP will add Operating Systems and Databases to this tracking list so all can be tracked from one source. This will be completed by the end of Q1 2017.*
2. *At the end of each annual budget cycle, IT management reviews the list from #1 above for all platforms, infrastructure, applications, and software that need to be upgraded in the next calendar year. This list is sorted from highest to lowest priority.*
3. *IT management then submits a proposal to the Infrastructure Investment Review Board (IIRB) requesting funding for the items on the list.*
4. *Once funding is approved, the funds are used to upgrade as many items as possible starting with the high priority items.*

Recommendation 5 – Network Security: Network Access Controls

We recommend that DHP implement network access controls to prevent non-company owned devices from connecting to its internal network.

DHP Response:

DHP agrees with the recommendation.

A security solution has been purchased. Implementation of a network access controls project will begin in early 2017 but due to the complexity of the scope a definite planned completion date cannot be determined at this time. As this project progresses DHP will be in a better position to narrow down a planned completion time.

Recommendation 6 – Configuration Management: Security Configuration Standards

We recommend that DHP document approved security configuration settings for all operating platforms and databases deployed in its technical environment.

DHP Response:

DHP agrees with the recommendation.

DHP will document all database and operating system security configuration standards by the end of Q3 2017.

Recommendation 7 – Configuration Management: Security Configuration Auditing

We recommend that DHP implement a process to routinely audit the configuration settings of servers and databases to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

DHP Response:

DHP agrees with this recommendation.

Once the database and operating system security configuration standards have been documented (see #6), DHP will implement processes to audit these settings to make sure they are in compliance with the approved standards.

Recommendation 8 – Application Controls: Claims Processing – Paper Claims Tracking

We recommend that DHP implement a process to verify that all paper claims are tracked throughout the claims adjudication process.

DHP Response:

DHP agrees with the recommendation.

DHP has implemented the following to address the recommendation:

1. *DHP now uses locked containers for transporting paper claims between buildings.*
2. *Each container will have a log sheet showing* [redacted] *The same process is followed when claims are being returned to the mail room.*
3. *Security for the mail room at* [redacted] *has been upgraded to require* [redacted] *for entry. Access to the mail room is limited to authorized staff only.*

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