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

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF NEBRASKA

Report Number 1A-10-53-17-042
April 17, 2018

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Blue Cross Blue Shield of Nebraska

Report No. 1A-10-53-17-042 **April 17, 2018**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of Nebraska (BCBSNE) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

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

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- BCBSNE has established an adequate security management program.
- BCBSNE has adequate physical access controls for its facilities and data centers. Furthermore, BCBSNE has adequate logical access controls protecting sensitive data in its network environment.
- BCBSNE does not have adequate security controls in place within its internal network to manage traffic between [redacted].
- BCBSNE does not conduct routine vulnerability scanning of its web application. Furthermore, BCBSNE does not have a formal process to ensure that vulnerabilities identified from vulnerability scanning are remediated in a timely manner.
- BCBSNE has not documented security configuration standards for all of the operating platforms in its network environment. Furthermore, BCBSNE's subsidiary, [redacted], does not maintain security configuration standards for the mainframe that hosts BCBSNE's claims processing system.
- BCBSNE has not tested the connection with [redacted]'s backup data center in the event that the [redacted]'s primary data center becomes unavailable to process FEHBP claims.
- BCBSNE has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

BCBSND	**Blue Cross Blue Shield of North Dakota**
BCBSNE	**Blue Cross Blue Shield of Nebraska**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Security Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
LAN	**Local Area Network**
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**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Blue Cross Blue Shield of Nebraska (BCBSNE).

The audit was conducted pursuant to FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

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

This was our first audit of BCBSNE's information technology (IT) general and application controls. All BCBSNE 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 BCBSNE's IT environments. We accomplished these objectives by reviewing the following areas:

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

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 BCBSNE's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of BCBSNE'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 BCBSNE to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Omaha, Nebraska and Fargo, North Dakota.

BCBSNE's claims processing application is hosted by [redacted], a jointly-owned subsidiary of BCBSNE and Blue Cross Blue Shield of North Dakota (BCBSND). [redacted] is responsible for maintaining the mainframe on which the claims processing application resides. The operations of [redacted] were considered within the scope of this audit.

The onsite portion of this audit was performed in June and July of 2017. We completed additional audit work before and after the on-site visits 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 BCBSNE as of July 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSNE. 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 BCBSNE's business structure and environment;

- Performed a risk assessment of BCBSNE'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 BCBSNE'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;

- Control Objectives for Information and Related Technologies 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, Revision 1, An Introduction to Information 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, Revision 1, Guidelines on Firewalls and Firewall Policy;

- NIST SP 800-44, Version 2, Guidelines on Securing Public Web Servers;

- 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 BCBSNE’s practices were consistent with applicable standards. While generally compliant with respect to the items tested, BCBSNE was not in complete compliance with all standards, as described in section III 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 BCBSNE's overall IT security program. We evaluated BCBSNE's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

BCBSNE has documented policies that outline its enterprise security management framework. BCBSNE has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSNE also has implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BCBSNE 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 at BCBSNE's facilities and data centers. Additionally, we reviewed physical access and environmental controls at [redacted] data center that hosts BCBSNE's claims processing application. We also examined the logical access controls protecting sensitive data in BCBSNE's network environment and claims processing related applications.

The access controls observed during this audit included, but were not limited to:

- Procedures for appropriately granting, adjusting, and removing physical access to facilities and data centers;

- Procedures for appropriately granting, adjusting, and removing logical access to information systems; and

- Robust physical and environmental controls within BCBSNE's and BCBSND's data centers.

Nothing came to our attention to indicate that BCBSNE does not have adequate access controls.

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 BCBSNE'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 documented incident response program.

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

1) Internal Network Segmentation

Firewalls are used at key locations on BCBSNE's network in order to control connections with systems outside of its network. Virtual LANs are used to internally segment portions of BCBSNE's network. However, virtual LAN's alone are not an adequate security control to manage traffic between different portions of a network.

BCBSNE does not have adequate security controls to segregate [redacted] segments.

NIST SP 800-41, Revision 1, advises that, "Focusing attention solely on external threats leaves the network wide open to attacks from within. These threats may not come directly from insiders, but can involve internal hosts infected by malware or otherwise compromised by external attackers. Important internal systems should be placed behind internal firewalls."

Failure to segregate [redacted] segments increases the risk that a system could be compromised and allow access to sensitive servers and data.

Recommendation 1

We recommend that BCBSNE implement security controls (e.g., firewalls) within its internal network in order to adequately segregate sensitive resources from [redacted] systems.

BCBSNE Response:

"BCBSNE agrees with the recommendation. Steps have been taken to create a roadmap to further separate sensitive resources from [redacted] systems. This initiative will be completed by June 30, 2019."

OIG Comment:

As a part of the audit resolution process, we recommend that BCBSNE 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 audit report that BCBSNE agrees to implement.

2) Web Application Scanning

BCBSNE maintains a public-facing member web portal. When the application was first developed, BCBSNE performed an automated scan on the web application to test for vulnerabilities. BCBSNE recently implemented a policy requiring a vulnerability scan after any significant change is made to the web application. However, if there are no changes, the web application is not subject to any additional security testing.

NIST SP 800-44, Version 2, states that "Periodic security testing of public Web servers is critical." NIST SP 800-44, Version 2, also states that "Vulnerability scanning assists a Web server administrator in identifying vulnerabilities and verifying whether the existing security measures are effective." Failure to periodically test a web application for vulnerabilities increases the risk that unidentified weaknesses could be exploited.

Recommendation 2

We recommend that BCBSNE update its scanning process to ensure that credentialed vulnerability scans are routinely conducted on web applications.

BCBSNE Response:

"BCBSNE agrees with this recommendation. BCBSNE has reviewed and updated its policy and procedure, verifying that credentialed vulnerability scanning occurs on a quarterly basis, and/or after significant changes to the environment on October 31, 2017."

OIG Comment:

In response to the draft audit report, we received an updated Vulnerability Assessment Procedure that mandates quarterly vulnerability scans on web applications. We also reviewed the results of a recent web application vulnerability scan. No further action is required.

3) Vulnerability Management Program

BCBSNE conducts credentialed vulnerability scans on all servers in its network environment on a routine basis. Although the results of the scans are reviewed by security personnel, BCBSNE does not have a process in place to track the status of vulnerabilities identified by the scans to ensure they are remediated in a timely manner.

FISCAM states that, "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective." Additionally, NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities in a timely manner increases the risk that bad actors could exploit system weaknesses for malicious purposes.

Recommendation 3

We recommend that BCBSNE implement a process to ensure that vulnerabilities identified from vulnerability scanning are remediated in a timely manner.

<u>BCBSNE Response:</u>

"BCBSNE agrees with this recommendation. BCBSNE will formalize the processes to identify, coordinate, and track remediation of vulnerabilities identified during vulnerability scanning. The target date for completion is June 30, 2018."

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 BCBSNE's management of the configuration of its servers and databases. Our review found the following controls in place:

BCBSNE and [redacted] do not have documented security configuration standards for all operating platforms in use.

- Documented configuration management policies;
- System configuration changes are documented; and
- A formal change approval process.

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

1) Security Configuration Standards

BCBSNE has documented security configuration standards for most of its network environment. The security configuration standards were developed using Center for Internet Security benchmarks as guidance. However, approved configuration standards have not been documented for all of the operating platforms in BCBSNE's network environment. Furthermore, BCBSNE's subsidiary, [redacted], does not maintain configuration standards for the mainframe that hosts the BCBSNE claims processing system.

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 that the system may not be configured in a secure manner.

Recommendation 4

We recommend that BCBSNE document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

BCBSNE Response:

"BCBSNE agrees with this recommendation. Security configuration standards have been updated, approved, and implemented for technical assets used on BCBSNE enterprise networks, to include Operating System (OS) platforms and databases deployed throughout the technical environment as of December 31, 2017."

OIG Comment:

In response to the draft audit report, we received approved security configuration standards for all but one operating system. We recommend that BCBSNE provide OPM's Healthcare and Insurance Audit Resolution Group with the approved security configuration standard for the remaining operating system in BCBSNE's network environment.

Recommendation 5

We recommend that BCBSNE ensure that [redacted] document approved security configuration standards for its mainframe.

BCBSNE Response:

"BCBSNE agrees with this recommendation. [redacted] ***has developed a security configuration standard based on a Defense Information Systems Agency (DISA) Mainframe Product Security Requirements Guide as of January 15, 2018."***

2) Security Configuration Auditing

As noted above, BCBSNE and [redacted] have not documented approved security configuration standards for all operating platforms and databases deployed in their technical environments. Without approved security configuration standards BCBSNE and [redacted] cannot effectively audit their system's security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization 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 configuration compliance auditing program increases the risk that servers and the mainframe are not configured appropriately and left undetected can create a potential gateway for unauthorized access or malicious activity.

<u>Recommendation 6</u>

We recommend that BCBSNE implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 4 are in place.

<u>BCBSNE Response:</u>

"BCBSNE agrees with this recommendation. BCBSNE will implement technical solutions and complementary procedures to allow for scanning of the BCBSNE technical environment to confirm adherence to accepted security configuration standards. The target date for completion is June 30, 2018."

<u>Recommendation 7</u>

We recommend that BCBSNE ensure that [redacted] implement a process to routinely audit the configuration settings of the mainframe to ensure it is in compliance with the approved configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 5 are in place.

<u>BCBSNE Response:</u>

"BCBSNE agrees with this recommendation. [redacted] has completed the purchase and the implementation of a compliance monitoring software application as of January 31, 2018. The software will be utilized by [redacted] to assess the security of the mainframe

environment and compare compliance to the mainframe security configuration standard noted in the response for recommendation 6."

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 BCBSNE's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

BCBSNE and [redacted] have not tested the connection with the disaster recovery site for its claims processing application.

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Contingency plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." BCBSNE has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources. However, we noted one opportunity for improvement related to BCBSNE's contingency planning program.

1) Alternative Processing Site Connection

As mentioned in the scope and methodology section of this report, [redacted] hosts the claims processing application that BCBSNE uses to process FEHBP claims. [redacted] contracts with another vendor, [redacted], to host a recovery site for the claims processing application in the event that [redacted]'s facility and resources are unavailable. A network connection has been established between [redacted] and BCBSNE in the event that [redacted] is unavailable.

However, the network connection between BCBSNE and [redacted] has not been tested in order to ensure that BCBSNE has the ability to process Federal Employee Program (FEP) claims in the event that a network connection to [redacted] becomes unavailable.

NIST SP 800-53, Revision 4, states, "The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions." Furthermore, NIST SP 800-53, Revision 4, states, "The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing."

Failure to test the connection between BCBSNE and [redacted] increases the risk that BCBSNE will not meet its recovery time objectives for critical business functions if [redacted]'s facility and resources become unavailable.

<u>Recommendation 8</u>

We recommend that BCBSNE, [redacted], and [redacted] conduct a functional disaster recovery test of the network connection between BCBSNE and [redacted] to ensure that business operations at BCBSNE can continue in the event that [redacted]'s claims processing application is unavailable.

<u>BCBSNE Response:</u>

"BCBSNE, [redacted], and [redacted] will conduct a functional disaster recovery test of the network connection between BCBSNE and [redacted] to ensure that business operations at BCBSNE can continue in the event that [redacted]'s claims processing application is unavailable. This test will be completed by April 30, 2018."

F. <u>CLAIMS ADJUDICATION</u>

The following sections detail our review of the applications and business processes supporting BCBSNE's claims adjudication process. BCBSNE prices and adjudicates claims using a locally operated claims processing system maintained by [redacted] and then through the Blue Cross Blue Shield Association's nationwide FEP Direct claims processing system. We reviewed the following processes related to the claims adjudication process: application configuration management, claims processing, and provider debarment.

1) Application Configuration Management

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

BCBSNE and [redacted] have implemented policies and procedures related to application configuration management, and have also adopted a system development life cycle methodology that personnel follow during routine software modifications. We observed the following controls related to testing and approval of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;
- Unit, system, and user acceptance testing are conducted in accordance with a documented testing strategy; 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 BCBSNE and [redacted] have not implemented adequate controls related to the application configuration management process.

2) Claims Processing System

We evaluated the business process controls associated with BCBSNE's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that BCBSNE has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;
- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and
- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that BCBSNE has not implemented adequate controls over its claims processing systems.

3) Debarment

BCBSNE has adequate procedures for updating its claims system with debarred provider information. BCBSNE is notified by the Blue Cross Blue Shield Association that an update to the OPM OIG debarment list is available. BCBSNE personnel review the list to determine if any debarred providers have active contracts with BCBSNE. If an active provider is determined to be debarred, the provider is flagged in the FEP Direct system, which will cause any incoming claims to defer for further review. Furthermore, an email is sent to [redacted] to request termination of the debarred provider in the local claims processing system. BCBSNE adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

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

4) Application Controls Testing

We conducted a test of BCBSNE's claims adjudication application to validate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which BCBSNE's system adjudicated the claims. Our test results did not identify any issues.

APPENDIX

February 5, 2018

BlueCross BlueShield
Association

An Association of Independent
Blue Cross and Blue Shield Plans

Federal Employee Program
1310 G Street, N.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

[redacted], Auditor-in-Charge
Claims & IT Audits Group,
U.S. Office of Personnel Management (OPM)
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT IT AUDIT REPORT
Blue Cross Blue Shield of Nebraska (BCBSNE)
Audit Report Number 1A-10-53-17-042
(Dated December 13, 2017)

The following represents the Plan's response as it relates to the recommendations included in the draft report.

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

No recommendation noted.

C. NETWORK SECURITY

1. Internal Network Segmentation

Recommendation 1

We recommend that BCBSNE segregate its internal network in order to separate sensitive resources from [redacted] systems.

Plan Response

BCBSNE agrees with the recommendation. Steps have been taken to create a roadmap to further separate sensitive resources from [redacted] systems. This initiative will be completed by June 30, 2019.

2. Web Application Scanning

Recommendation 2

We recommend that BCBSNE update its scanning process to ensure that credentialed vulnerability scans are routinely conducted on web applications.

Plan Response

BCBSNE agrees with this recommendation. BCBSNE has reviewed and updated its policy and procedure, verifying that credentialed vulnerability scanning occurs on a quarterly basis, and/or after significant changes to the environment on October 31, 2017.

3. Vulnerability Management Program

Recommendation 3

We recommend that BCBSNE implement a process to ensure that vulnerabilities identified from vulnerability scanning are remediated in a timely manner.

Plan Response

BCBSNE agrees with this recommendation. BCBSNE will formalize the processes to identify, coordinate, and track remediation of vulnerabilities identified during vulnerability scanning. The target date for completion is June 30, 2018.

D. CONFIGURATION MANAGEMENT

1. Security Configuration Standards

Recommendation 4

We recommend that BCBSNE document approved security configuration standards for all operating system platforms and databases deployed in its technical environment.

Plan Response

BCBSNE agrees with this recommendation. Security configuration standards have been updated, approved, and implemented for technical assets used on BCBSNE enterprise networks, to include Operating System (OS) platforms and databases deployed throughout the technical environment as of December 31, 2017.

Recommendation 5

We recommend that BCBSNE ensure that [redacted] document approved security configuration standards for its mainframe.

Plan Response

BCBSNE agrees with this recommendation. [redacted] has developed a security configuration standard based on a Defense Information Systems Agency (DISA) Mainframe Product Security Requirements Guide as of January 15, 2018.

2. Security Configuration Auditing

Recommendation 6

We recommend that BCBSNE implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved configuration standards.

Note – this recommendation cannot be implemented until the controls from Recommendation 5 are in place.

Plan Response

BCBSNE agrees with this recommendation. BCBSNE will implement technical solutions and complementary procedures to allow for scanning of the BCBSNE technical environment to confirm adherence to accepted security configuration standards. The target date for completion is June 30, 2018.

Recommendation 7

We recommend that BCBSNE ensure that [redacted] implement a process to routinely audit the configuration settings of the mainframe to ensure it is in compliance with the approved configuration standards.

Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

Plan Response

BCBSNE agrees with this recommendation. [redacted] has completed the purchase and the implementation of a compliance monitoring software application as of

January 31, 2018. The software will be utilized by [redacted] to assess the security of the mainframe environment and compare compliance to the mainframe security configuration standard noted in the response for recommendation 6.

E. CONTINGENCY PLANNING

1. Alternative Processing Site Connection

Recommendation 8

We recommend that BCBSNE, [redacted], and [redacted] conduct a functional disaster recovery test of the network connection between BCBSNE and [redacted] to ensure that business operations at BCBSNE can continue in the event that [redacted]'s claims processing application is unavailable.

Plan Response

BCBSNE, [redacted], and [redacted] will conduct a functional disaster recovery test of the network connection between BCBSNE and [redacted] to ensure that business operations at BCBSNE can continue in the event that [redacted]'s claims processing application is unavailable. This test will be completed by April 30, 2018.

F. Claims Adjudication

No recommendation noted.

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [redacted] or [redacted] at [redacted].

Sincerely,

[redacted]
Executive Director, FEP Program Integrity

cc: [redacted], OPM
[redacted], FEP

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