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

Final Audit Report

Subject:

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUECROSS BLUESHIELD OF TENNESSEE

Report No. 1A-10-15-13-002

Date: August 6, 2013

Audit Report

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
BLUECROSS BLUESHIELD OF TENNESSEE
PLAN CODES 10 / 11
CHATTANOOGA, TENNESSEE

Report No. 1A-10-15-13-002

Date: August 6,2013

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM
CONTRACT 1039
BLUECROSS BLUESHIELD OF TENNESSEE
PLAN CODES 10 / 11
CHATTANOOGA, TENNESSEE

Report No. 1A-10-15-13-002

Date: August 6, 2013

This final report discusses the results of our audit of general and application controls over the information systems at BlueCross BlueShield of Tennessee (BCBST.)

Our audit focused on the claims processing applications used to adjudicate Federal Employees Health Benefits Program (FEHBP) claims for BCBST, as well as the various processes and information technology (IT) systems used to support these applications. We documented controls in place and opportunities for improvement in each of the areas below.

Security Management

BCBST has established a series of IT policies and procedures to create an awareness of IT security. We also verified that BCBST has adequate human resources policies related to the security aspects of hiring, training, transferring, and terminating employees.

Access Controls

BCBST has implemented numerous controls to grant, remove, and control physical access to its data center, as well as logical controls to protect sensitive information. We also noted various controls over physical access to the facilities, as well as the method for encrypting emails containing sensitive information.

Network Security

BCBST has documented network infrastructure diagrams, implemented a secure firewall architecture, maintains comprehensive incident response policies and procedures and utilizes software packages for incident correlation. However, BCBST's controls to detect rogue devices connected to its network could be improved.

Configuration Management

BCBST has developed formal policies and procedures that provide guidance for system software management and controlling configuration changes. However, we noted several weaknesses in BCBST's configuration management program related to system configuration auditing and its vulnerability scanning methodology.

Contingency Planning

We reviewed BCBST's business continuity plans and concluded that they contained the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis.

Claims Adjudication

BCBST has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. We also determined that BCBST has adequate policies and procedures related to application change control.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that BCBST is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Contents

Page

Executive Summary i

I. Introduction 1

Background 1

Objectives 1

Scope 2

Methodology 2

Compliance with Laws and Regulations 3

II. Audit Findings and Recommendations 4

A. Security Management 4

B. Access Controls 4

C. Network Security 4

D. Configuration Management 6

E. Contingency Planning 10

F. Claims Adjudication 11

G. Health Insurance Portability and Accountability Act 12

III. Major Contributors to This Report 13

Appendix: BlueCross BlueShield of Tennessee's March 11, 2013 response to the draft audit report issued January 10, 2013.

I. Introduction

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 BlueCross BlueShield of Tennessee (BCBST).

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.

Background

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

This was our first audit of BCBST's general and application controls. We also reviewed BCBST's compliance with the Health Insurance Portability and Accountability Act (HIPAA).

All BCBST 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.

Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in BCBST's IT environment.
We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Segregation of duties;
- Contingency planning;
- Application controls specific to BCBST's claims adjudication systems; and,
- HIPAA compliance.

Scope

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 BCBST'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 BCBST'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 BCBST to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. The business processes reviewed are primarily located in BCBST's Chattanooga, Tennessee facilities.

The on-site portion of this audit was performed in October and November of 2012. 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 BCBST as of November 2012.

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

Methodology

In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed BCBST's business structure and environment;
- Performed a risk assessment of BCBST'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. Results of samples that are judgmentally selected cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

Various laws, regulations, and industry standards were used as a guide to evaluating BCBST's control structure. These criteria include, but are not limited to, the following publications:

- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP 800-61, Computer Security Incident Handling Guide;
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule; and,
- HIPAA Act of 1996.

Compliance with Laws and Regulations

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

II. Audit Findings and Recommendations

A. Security Management

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

BCBST has implemented a series of formal policies and procedures that comprise its security management program. BCBST's Information Security Committee is responsible for creating, reviewing, editing, and disseminating IT security policies. BCBST has also developed a thorough risk management methodology, and has procedures to document, track, and mitigate or accept identified risks. We also reviewed BCBST's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BCBST 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 several BCBST facilities and data centers. We also examined the logical controls protecting sensitive data on BCBST's network environment and claims processing 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 recertifying access to data centers and restricted areas;
- Procedures for removing Windows/network access for terminated employees; and,
- Controls to monitor and filter email and Internet activity.

Nothing came to our attention to indicate that BCBST has not implemented adequate controls related to logical or physical access.

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.

BCBST has documented thorough and complete network infrastructure diagrams. BCBST has implemented a secure firewall architecture in its network and conducts routine configuration reviews of these devices. BCBST's incident response policies and procedures are

comprehensive, and they utilize software packages for incident correlation. However, BCBST's controls to detect rogue devices connected to its network could be improved.

1. Detecting Rogue Network Devices

BCBST has not implemented technical controls to prevent rogue devices (workstations not issued or approved by the company) from connecting to its network.

NIST SP 800-53 Revision 3 requires that an information system uniquely identify and authenticate before establishing a connection. Failure to detect rogue devices increases the risk that an insecure device could connect to the network. For example, any employee could connect a personal laptop with viruses or a malicious employee could connect a device with hacking tools.

Recommendation 1

We recommend that BCBST implement controls to prevent rogue devices from connecting to its network.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that there are numerous compensating controls in place for system security that they believe sufficiently address this recommendation. These controls were in place prior to the start of this audit. Appendix A provides details of the technical controls in place to prevent rogue devices from connecting to BCBST networks."

OIG Reply:

While we acknowledge the benefits of the five controls listed in Appendix A of the BCBST response, they are not sufficient to prevent rogue devices from connecting to its network.

Each of the controls listed in Appendix A of the BCBST response to the draft are addressed below:

1. **Disabled Network Ports**. Disabling network ports in the public and general access areas, while a good control to have in place, does not prevent an authorized employee with access to BCBST facilities from connecting a rogue device to the BCBST network at an employee workstation.
2. **Intrusion Detection System**. A behavioral intrusion detection system could potentially flag malicious activity from a rogue device, but does not prevent the rogue device from being connected to the network in the first place, and does not prevent malicious attacks from executing.
3. **Signature-based Intrusion Prevention System (IPS)**. As with an intrusion detection system, an IPS does nothing to prevent rogue devices from connecting to the network. We do agree that this control could potentially stop some malicious attacks, but also note that many hacking tools are designed to elude an IPS, and continue to believe that additional controls should be implemented to prevent unauthorized devices from connecting to the network.

4. **Wireless IPS**. A wireless IPS can reduce the threat of malicious attacks via wireless connections, but does nothing to address rogue devices physically connected to the network.
5. **Physical Security**. BCBST's physical access controls reduce the risk of unauthorized individuals accessing the company's facilities, but it does not address the risk of employees connecting rogue devices to the network.

This is a standard control observed at many FEHBP carriers. We continue to recommend that BCBST implement the technical controls to prevent rogue devices from connecting to its network.

D. Configuration Management

We evaluated BCBST's management of the configuration of its claims processing application and the server and mainframe environments that support it, and determined that the following controls were in place:

- Approved server configuration images;
- Controls for monitoring privileged user activity on the operating platform; and
- Thorough change management procedures for system software.

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

1. Baseline Configuration Policy

BCBST has created baseline configuration images for its server environment. However, BCBST has not created baseline configuration documentation for its mainframe security software installation.

NIST SP 800-53 Revision 3 states that an organization must develop, document, and maintain a current baseline configuration of the information system. NIST SP 800-53 Revision 3 also 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. BCBST cannot effectively audit its mainframe security settings without a baseline, as the baseline should be the basis for comparison.

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

Recommendation 2

We recommend that BCBST document approved mainframe security settings.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that Mainframe Support and Information Security Operations staff determined the appropriate configuration settings to include in a SETR (mainframe security settings) baseline configuration. BCBST management approved the baseline for the mainframe security settings on February 21, 2013. The details of the changes implemented are outlined in Appendix B."

OIG Reply:

The evidence provided by BCBST in response to the draft audit report indicates that BCBST has made the appropriate changes to their mainframe configuration settings; no further action is required.

Recommendation 3

We recommend that BCBST routinely audit mainframe settings to ensure they are in compliance with the approved baseline.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that staff will implement an automated process, which will compare approved baseline settings against current SETR configuration. This implementation is scheduled to be completed by April 30, 2013."

OIG Reply:

As part of the audit resolution process, we recommend that BCBST update OPM's Healthcare and Insurance Office (HIO) on its progress to document the approved mainframe configuration settings.

2. Mainframe System Configuration

We reviewed BCBST's actual mainframe configuration and identified insecure settings. The problems we detected were provided to BCBST during the fieldwork phase of the audit and related to settings for resource auditing. However, due to the sensitive nature of these findings, the specific settings in question will not be included in this report. BCBST reviewed our findings and stated that it will conduct testing of the settings during the first quarter of 2013 and, if no adverse impact is detected, implement production changes by March 31, 2013.

Recommendation 4

We recommend that BCBST make the appropriate configuration changes related to the specific weaknesses identified during this audit.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that Information Security Operations staff reviewed the configuration setting in question and determined it would no longer create performance issues within our mainframe environment as previously determined. In order to implement the

appropriate configuration changes, testing of this setting will be performed during the first quarter of 2013. If no adverse impact is detected, production implementation will occur by March 31, 2013."

OIG Reply:

As part of the audit resolution process, we recommend that BCBST update OPM's HIO on its progress to implement the configuration changes addressed in this recommendation.

3. Vulnerability Scanning

We reviewed BCBST's vulnerability scanning process and conducted our own independent vulnerability scans on BCBST's information systems, using automated tools. We identified several areas for improvement.

Documented Accepted Vulnerabilities

BCBST conducts periodic vulnerability scans on its information systems using automated tools, and contracts a third party vendor to conduct external scans. Identified vulnerabilities are reviewed to determine the necessary steps to remediate the weaknesses. In the event there is a business reason a vulnerability cannot be addressed, the weakness is accepted by management. However, BCBST does not have a formal process for documenting, tracking, or reviewing these known and accepted vulnerabilities.

NIST SP 800-53 Revision 3 states that an organization identify, document, and approve exceptions from mandatory configuration settings for individual components within the information system based on explicit operational requirements.

Failure to track accepted weaknesses decreases an organization's ability to protect itself and increases its risk of being attacked by a malicious user looking to exploit these identified vulnerabilities.

Recommendation 5

We recommend that BCBST implement a formal process to document, track, and review accepted vulnerabilities identified during vulnerability and compliance scanning.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that staff will continue with a manual process for vulnerability and patch management until a formal process can be implemented. Staff will define a plan to expand existing processes to utilize commercial software products for automated support of vulnerability and patch management. The details of the plan are scheduled to be finalized by June 30, 2013."

OIG Reply:

As part of the audit resolution process, we recommend that BCBST update OPM's HIO on its incremental progress to develop a plan and policy to automate the tracking of vulnerabilities. Ultimately, we recommend that BCBST provide evidence of the full

implementation of the commercial software product to automate tracking of vulnerabilities identified during vulnerability and compliance scanning for closure of this recommendation.

System Patching

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

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 3 states "The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously."

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

Recommendation 6

We recommend that BCBST improve its procedures and controls to ensure that production servers are installed with appropriate patches, service packs, and hot fixes on a timely basis.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that upon completion of the implementation plan, staff will have better assurance that appropriate patches, service packs, and hot fixes are installed on a timely basis. The changes will include the development of procedures and controls to enhance the patch management process."

OIG Reply:

As part of the audit resolution process, we recommend that BCBST update OPM's HIO on its incremental progress to develop a plan and policy to automate patch management. Ultimately, we recommend that BCBST provide evidence of the full implementation of the commercial software product to ensure that production servers are installed with appropriate patches, service packs, and hot fixes on a timely basis.

Noncurrent Software

The results of our vulnerability scans indicated that several servers contained noncurrent software applications that were no longer supported by the vendors and have known security vulnerabilities.

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

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

Recommendation 7

We recommend that BCBST implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

BlueCross BlueShield of Tennessee Response:

"The Plan stated that non-current software will be identified during the patch management process and tracked in a BCBST approved repository. A risk acceptance determination will be reviewed and documented by management to facilitate a disposition to the non-current software."

OIG Reply:

As part of the audit resolution process, we recommend that BCBST provide OPM's HIO with evidence of its improved methodology to ensure only current and supported versions of system software are installed on the production servers.

E. Contingency Planning

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

- Disaster response plan;
- Business continuity plan for data center operations;
- Business continuity plans for claims processing operations and claims support;
- Disaster recovery plan tests conducted in conjunction with the alternate data center; and,
- Emergency response procedures and training.

We determined that the Plan's contingency planning documentation contained the critical elements suggested by NIST SP 800-34, "Contingency Planning Guide for IT Systems." BCBST 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, one area for improvement was noted during our review of BCBST's data center.

1. Diesel Generator

The Plan does not have a contract in place to provide diesel fuel for the generators supporting the data center in the event of a disaster. Once the fuel stored on-site has been utilized, BCBST does not have a guaranteed fuel supply and thus cannot ensure the continued operations of its data center in the event of a disaster.

NIST SP 800-34 states that "A combination UPS/generator system can provide clean, secure power for a system as long as fuel is available for the generator. Fuel availability should be considered for those who opt for a UPS/generator to support their system environment."

The lack of guaranteed fuel delivery in the event of a disaster increases the likelihood that BCBST will not be able to maintain data center operations during long term power outages.

Recommendation 8

We recommend that BCBST re-evaluate its diesel generator resources and make the appropriate changes to ensure its ability to maintain data center operations in the event of a long term power loss.

BlueCross BlueShield of Tennessee Response:

"The Plan has a diesel storage capacity of 20,000 gallons (2 - 10,000 gallon tanks). The generators burn 110 gallons per hour at full load, which equates to 2,640 gallons per 24 hours per generator. BCBST currently utilizes two generators. Based upon the information presented above, BCBST has the capacity to operate both generators at full load for approximately four days. In addition, staff has determined that there would be sufficient diesel fuel on hand in case of an emergency. However, to solidify this process and to address the OPM recommendation, the Plan has obtained a signed commitment from a local diesel fuel supplier to provide necessary deliveries in the event of an emergency. Appendix C provides the details of this agreement."

OIG Reply:

The evidence provided by BCBST in response to the draft audit report indicates that BCBST now maintains a sufficient agreement for the delivery of diesel fuel in the event of a disaster; no further action is required.

F. Claims Adjudication

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

1. Application Configuration Management

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

BCBST 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:

- BCBST 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,
- BCBST uses a business unit independent from the software developers to move the code between the development and production environments to ensure adequate segregation of duties.

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

2. Claims Processing System

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

- Paper claims that are received in the mail room are tracked to ensure timely processing;
- Claims are monitored as they are processed through the systems 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 BCBST has not implemented adequate controls over the claims processing system.

3. Debarment

BCBST has adequate procedures for updating its claims processing systems with debarred provider information, and routinely audits its debarment database for accuracy.

BCBST downloads the OPM OIG debarment list every month and compares it to its own provider database. Providers that are a direct match to the debarment list are automatically flagged in the provider database. A manual review is conducted for all partial matches to ensure that all debarred providers are appropriately terminated.

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

G. Health Insurance Portability and Accountability Act

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

BCBST has implemented a series of IT security policies and procedures to adequately address the requirements of the HIPAA security rule. BCBST has also developed a series of privacy policies and procedures that directly addresses all requirements of the HIPAA privacy rule. BCBST reviews its HIPAA privacy and security policies annually and updates them when necessary. BCBST's HIPAA organization is divided into three functional areas that have the responsibility of ensuring compliance with HIPAA Privacy and Security policies. Each year, all employees must complete compliance training which encompasses HIPAA regulations as well as general compliance.

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

III. Major Contributors to This Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Deputy Assistant Inspector General for Audits
- [redacted], Senior Team Leader
- [redacted], Auditor-In-Charge
- [redacted], IT Auditor
- [redacted], IT Auditor

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans
Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

March 11, 2013

[redacted], Chief
Information Systems Audits Group
Insurance Service Programs
Office of Personnel Management
1900 E Street, N.W., Room 6400
Washington, D.C. 20415

Reference: OPM DRAFT EDP AUDIT REPORT
BlueCross BlueShield of Tennessee (BCBST)
Audit Report Number 1A-10-15-13-002
Report Dated January 10, 2013 and Received January 10, 2013

Dear [redacted]:

This report is in response to the above-referenced U.S. Office of Personnel Management (OPM) Draft Audit Report covering the Federal Employees Health Benefits Program (FEHBP) Audit of Information Systems General and Application Controls for the Plan's interface with the FEP claims processing system, access, and security controls. Our comments regarding the recommendations in this report are as follows:

A. NETWORK SECURITY

1. Network Port Scanning

Recommendation 1

The OIG Auditors recommend that BCBST implement controls to prevent rogue devices from connecting to its network.

Response to Recommendation 1

The Plan stated that there are numerous compensating controls in place for system security that they believe sufficiently address this recommendation. These controls were in place prior to the start of this audit. Appendix A provides details of the technical controls in place to prevent rogue devices from connecting to BCBST networks.

B. CONFIGURATION MANAGEMENT

1. Baseline Configuration Policy

Recommendation 2

The OIG Auditors recommend that BCBST document approved mainframe security settings.

Response to Recommendation 2

The Plan stated that Mainframe Support and Information Security Operations staff determined the appropriate configuration settings to include in a SETR (mainframe security settings) baseline configuration. BCBST management approved the baseline for the mainframe security settings on February 21, 2013. The details of the changes implemented are outlined in Appendix B.

Recommendation 3

The OIG Auditors recommend that BCBST routinely audit mainframe settings to ensure they are in compliance with the approved baseline.

Response to Recommendation 3

The Plan stated that staff will implement an automated process, which will compare approved baseline settings against current SETR configuration. This implementation is scheduled to be completed by April 30, 2013.

2. Mainframe System Configuration

Recommendation 4

The OIG Auditors recommend that BCBST make the appropriate configuration changes related to the specific weaknesses identified during this audit.

Response to Recommendation 4

The Plan stated that Information Security Operations staff reviewed the configuration setting in question and determined it would no longer create performance issues within our mainframe environment as previously determined. In order to implement the appropriate configuration changes, testing of this setting will be performed during the first quarter of 2013. If no adverse impact is detected, production implementation will occur by March 31, 2013.

3. Vulnerability Scanning

Recommendation 5

The OIG Auditors recommend BCBST implement a formal process to document, track, and review accepted vulnerabilities identified during vulnerability and compliance scanning.

Response to Recommendation 5

The Plan stated that staff will continue with a manual process for vulnerability and patch management until a formal process can be implemented. Staff will define a plan to expand existing processes to utilize commercial software products for automated support of vulnerability and patch management. The details of the plan are scheduled to be finalized by June 30, 2013.

Recommendation 6

The OIG Auditors recommend BCBST implement proper procedures and controls to ensure that production servers are installed with appropriate patches, service packs, and hot fixes on a timely basis.

Response to Recommendation 6

The Plan stated that upon completion of the implementation plan, staff will have better assurance that appropriate patches, service packs, and hot fixes are installed on a timely basis. The changes will include the development of procedures and controls to enhance the patch management process.

Recommendation 7

The OIG Auditors recommend BCBST implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

Response to Recommendation 7

The Plan stated that non-current software will be identified during the patch management process and tracked in a BCBST approved repository. A risk acceptance determination will be reviewed and documented by management to facilitate a disposition to the non-current software.

C. CONTINGENCY PLANNING

1. Diesel Generator

Recommendation 8

The OIG Auditors recommend that BCBST re-evaluate its diesel generator resources and make the appropriate changes to ensure its ability to maintain data center operations in the event of a long term power loss.

Response to Recommendation 8

The Plan has a diesel storage capacity of 20,000 gallons (2 - 10,000 gallon tanks). The generators burn 110 gallons per hour at full load, which equates to 2,640 gallons per 24 hours per generator. BCBST currently utilizes two generators. Based upon the information presented above, BCBST has the capacity to operate both generators at full load for approximately four days. In addition, staff has determined that there would be sufficient diesel fuel on hand in case of an emergency. However, to solidify this process and to address the OPM recommendation, the Plan has obtained a signed commitment from a local diesel fuel supplier to provide necessary deliveries in the event of an emergency. Appendix C provides the details of this agreement.

We appreciate the opportunity to provide our response to this Draft Audit Report and request that our comments be included in their entirety as an amendment to the Final Audit Report.

Sincerely,

[redacted]

[redacted], CPA
Director, Program Assurance

[redacted]

cc: [redacted], BCBST
[redacted], BCBST
[redacted], OPM