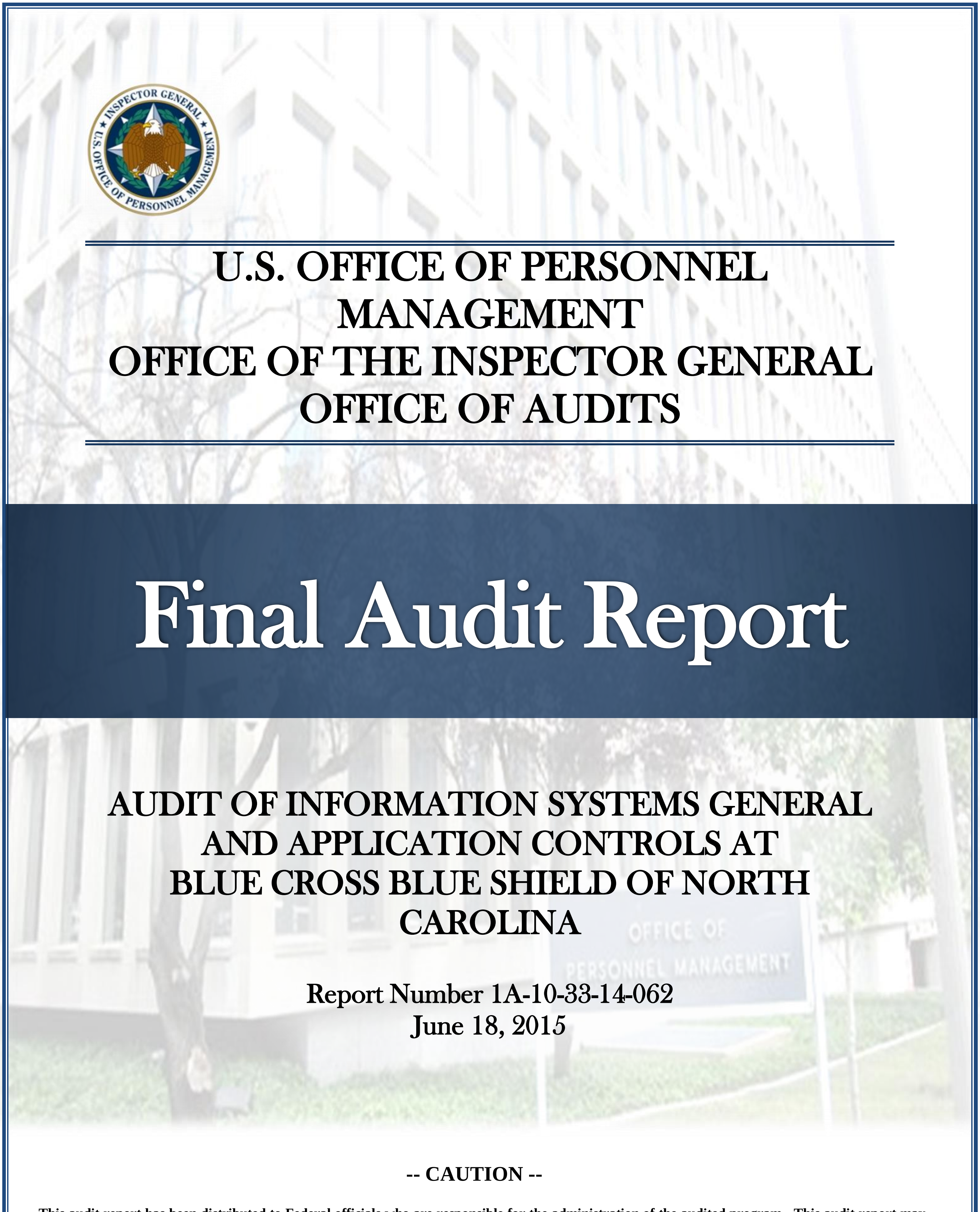

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF NORTH CAROLINA

Report Number 1A-10-33-14-062
June 18, 2015

-- CAUTION --

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

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Blue Cross Blue Shield of North Carolina

Report No 1A 10 33 14 062 **June 18, 2015**

Why Did We Conduct the Audit?

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of Federal Employee Health Benefit Plan (FEHBP) data processed and maintained in Blue Cross Blue Shield of North Carolina's (BCBSNC) information technology (IT) environment.

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- BCBSNC has established an adequate security management program.
- BCBSNC has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted several areas of concern related to BCBSNC's access controls:
  - There is no technical control to detect or prevent [redacted] at BCBSNC facilities.
  - The current process of reviewing physical access does not require managers to acknowledge the review.
- BCBSNC has implemented an incident response and network security program. However, we noted several areas of concern related to BCBSNC's network security controls:
  - A patch management policy is in place, but our test work identified several instances where patches are not being implemented in a timely manner.
  - Our test work indicated that [redacted] contained unsupported or out-of-date software.
- BCBSNC has developed formal configuration management policies and baselines for its operating platforms. Furthermore, BCBSNC has a documented change control process for the documented baseline configurations.
- BCBSNC's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. However, we noted two areas of concern related to BCBSNC's contingency planning controls:
  - BCBSNC does not verify with individual business units that appropriate business continuity plan testing has occurred.
  - BCBSNC's disaster recovery plan specific to its federal line of business does not include the necessary level of detail for testing.
- BCBSNC has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

the Act	The Federal Employees Health Benefits Act
BCBSA	Blue Cross Blue Shield Association
BCBSNC	Blue Cross Blue Shield of North Carolina
BCP	Business Continuity Plan
CFR	Code of Federal Regulations
FEHBP	Federal Employee’s Health Benefit Plan
FEP	Federal Employee Program
FISCAM	Federal Information Systems Control Audit Manual
GAO	U.S. Government Accountability Office
HIO	Healthcare and Insurance Office
HIPAA	Health Insurance Portability and Accountability Act
IT	Information Technology
NIST	National Institute of Standards and 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	Blue Cross Blue Shield of North Carolina

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 Blue Cross Blue Shield of North Carolina (BCBSNC or Plan).

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 (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 is our second audit of BCBSNC's information systems. The prior audit report (Report No. 1A-10-33-05-027, dated July 3, 2006) contained 15 recommendations. As part of this audit we followed up on the status of those prior recommendations and determined that they had all been adequately resolved.

All BCBSNC 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

Objective

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

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation of duties;
- Contingency planning; and
- Application controls specific to BCBSNC's claims processing systems.

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 BCBSNC's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of BCBSNC'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 BCBSNC to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. BCBSNC participates in a nationwide fee-for-service plan sponsored by the BlueCross and BlueShield Association's (BCBSA) Federal Employee Program (FEP). BCBSNC processes FEHBP claims through FEP Direct, the BCBSA's nation-wide claims adjudication system. The business processes reviewed are primarily located in BCBSNC's Chapel Hill and Durham, North Carolina facilities.

The on-site portion of this audit was performed in August and September of 2014. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSNC as of October 2014.

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

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

- Title 48 of the CFR;
- 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;
- Information Technology Governance Institute's COBIT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;

- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide; and
- NIST SP 800-66 Revision 1, An Introductory Resource Guide for Implementing the HIPAA Security Rule.

Compliance with Laws and Regulations

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

1. Security Management

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

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

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

Nothing came to our attention to indicate that BCBSNC does not have an adequate security management program.

2. 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 BCBSNC's facilities and data centers located in [redacted], North Carolina. We also examined the logical controls protecting sensitive data in BCBSNC's network environment and applications.

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

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

However, the following sections document opportunities for improvement related to BCBSNC's physical access controls.

a) Access to BCBSNC Facilities

BCBSNC's facilities use electronic card readers to control physical access. The BCBSNC data center has both card readers and biometric scanners. However, we expect all FEHBP contractors to also have some form of technical or physical control to detect or prevent [redacted].

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

Recommendation 1

We recommend that BCBSNC conduct a review of its physical access controls and implement some form of [redacted] prevention controls at its facility entrances.

Plan Response to Recommendation 1:

"In response to this recommendation, we have determined that the existing physical access controls are appropriate to minimize the likelihood of [redacted]. Currently, the plan has the following controls in place to enforce the physical access of our buildings: electronic security technology, on-site security personnel, badge readers, CCTV cameras, restricted access to restricted areas, security and safety policies and procedures, door alarms etc."

OIG Reply:

The physical access controls listed in the Plan's response above are not in place in every BCBSNC building. With the inconsistent implementation of controls, there is a significant risk of a physical access breach to areas of the BCBSNC facilities that contain sensitive information. A badge reader alone does not prevent [redacted] into the facility. At a minimum, a formal assessment should be done to consider the risks from unauthorized entry into BCBSNC facilities. We continue to recommend the implementation of technical controls to prevent [redacted] at all facility entrances.

b) Physical Access Recertification

BCBSNC's process for removing physical access to its facilities for terminated employees begins with the notification to building security of the expected termination date. On a monthly basis, lists of all employees with active access to secure areas are sent to the manager responsible for those areas for validation. The managers are told to respond if there is an issue with the physical access rights, but are not required to acknowledge the review if there are no issues.

However, BCBSNC's process for reviewing employees' physical access after termination could be improved. Access should be routinely reviewed for all physical access levels, not just for secure areas. Additionally, a written response from managers should be required to ensure that the full review is completed every month.

NIST SP 800-53 Revision 4 states that an organization must review and analyze system audit records for indications of inappropriate or unusual activity. Failure to remove and audit physical access to terminated users increases the risk that a terminated employee could enter a facility and steal, modify, or delete sensitive and proprietary information. Lack of a required confirmation from managers increases the risk that employees maintain improper access to BCBSNC facilities.

Recommendation 2

We recommend that BCBSNC implement a process to routinely audit all active access cards to ensure that they are not assigned to terminated employees; this process should include written confirmation from managers.

Plan Response to Recommendation 2:

"In response to this recommendation, The Plan agrees to investigate and improve its current process and remediate, as appropriate, second quarter, June 30, 2015."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSNC provide OPM's Healthcare and Insurance Office (HIO) evidence of the process change and of manager's review.

3. 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.

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

a) Vulnerabilities Identified in Automated Scans

We worked with BCBSNC employees to independently perform automated vulnerability scans on a sample of [redacted]. The results are outlined in the sections below.

System Patching

BCBSNC has documented patch management policies and procedures. However, the results of the vulnerability scans conducted during this audit indicate that [redacted] [redacted] were missing at least one critical patch or service

BCBSNC's failure to promptly install all important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

pack greater than 90 days old. BCBSNC did not provide evidence indicating that it was previously aware of these missing patches and had documented its acceptance of the associated risk.

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

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

Recommendation 3

We recommend that BCBSNC improve its procedures and controls to ensure that [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis.

Recommendation 4

We recommend that BCBSNC improve its procedures and controls to ensure that [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis.

Plan Response to Recommendations 3 & 4:

"BCBSNC Security Management meets with the Security Operations team weekly and monthly providing monitoring and oversight to ensure that the existing policies and procedures are being followed. Vulnerabilities are assessed for risk, assigned remediation timelines, and remediated according to the guidelines in the documented procedures. Application supportability and availability are factors that determine and possibly dictate timelines for deployment of patches, service packs, and hot fixes. In instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as [redacted] [redacted], [redacted], [redacted] and [redacted]. The Plan will utilize continuous improvement for all items related to securing our [redacted]. In addition, the Plan will continue to review and, if appropriate, update the established policies and procedures to ensure [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis or compensating controls are identified for significant risk items."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSNC provide OPM's HIO with evidence that it has implemented controls to ensure [redacted] are installed with appropriate patches, service packs and hotfixes on a timely basis. This evidence should include documentation (e.g., several iterations of vulnerability scan reports) indicating that [redacted] have remained up-to-date with patches.

Noncurrent Software

The results of the vulnerability scans also indicated that [redacted] contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities. BCBSNC did not provide any evidence indicating that it previously knew about the unsupported software and documented its acceptance of this risk.

[redacted] contained noncurrent software applications no longer supported by the vendors and known to have security vulnerabilities.

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

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

Recommendation 5

We recommend that BCBSNC implement a methodology to ensure that only current and supported versions of system software are installed [redacted].

Recommendation 6

We recommend that BCBSNC implement a methodology to ensure that only current and supported versions of system software are installed on [redacted]

Plan Response to Recommendations 5 & 6:

"BCBSNC is aware that some unsupported software runs on our network and agree it would be preferable for all software to be at current versions. There will be occasions where the Plan's business and Information Technology Group (ITG) departments partner to make risk-aware decisions to not upgrade or replace software. Software that is to become unsupported is inventoried and the impacts of upgrading, replacing, or accepting risk are discussed with business owners. Decisions to not upgrade low risk software may be based on business drivers such as 'Reliant applications are to be retired' or 'the Plan will pay for extended vendor support until internal resources are available for the upgrade'. In

instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as [redacted]***,*** [redacted]***,*** [redacted] ***and*** [redacted]

The Plan has a Technology Roadmap in place to address software and hardware currency. With this plan, unsupported software may be needed while ramping up the current software and hardware. For any unsupported software in place during the audit, compensating controls and alternate methods to mitigate any risks were in place and continue to be monitored. The Plan continues to look for methods to improve all items related to securing our [redacted]***."***

OIG Reply:

BCBSNC's response indicated that there are business needs that require the use of unsupported system software and that the Plan leverages third party security tools to mitigate risk. However, we believe that in spite of these compensating controls, this weakness poses a strong threat to the organization and increases the risk of a malicious attack exploiting these known vulnerabilities.

We continue to recommend that BCBSNC implement a methodology to routinely remove unsupported software from [redacted], and that this include a process for documenting known instances of non-compliance.

4. Configuration Management

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

- Documented corporate configuration policy;
- Documented baseline configurations for all operating systems; and
- Thorough change management procedures for system software and hardware.

Nothing came to our attention to indicate that BCBSNC has not implemented adequate controls over system software management.

BCBSNC maintains baseline configurations for all operating systems.

5. Contingency Planning

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

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

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems." BCBSNC 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.

a) Business Continuity Plan Tests

BCBSNC delegates the responsibility for conducting Business Continuity Plan (BCP) tests to the functional owners of each plan. Currently, there is no validation or review to ensure that testing of each BCP is conducted in accordance with BCBSNC regulation.

NIST 800-34 Revision 1 states that "Test results and lessons learned should be . . . reviewed by test participants and other personnel as appropriate." Failure to have managerial review of testing increases the risk that the organization will not be able to continue business operations when unexpected events occur.

Recommendation 7

We recommend BCBSNC document the business continuity tests results and implement a process for routine managerial review.

Plan Response to Recommendation 7:

"In response to this recommendation, the Plan agrees.

FEP business operations will conduct at least one physical test through either a call tree or tabletop exercise per year. Evidence of this exercise will be maintained within the FEP business operations area and reported to its Senior Leadership Team (SLT) representative and the Enterprise Business Continuity (EBC) Team.

Effective immediately, the Enterprise Business Continuity (EBC) Team will reinforce its current Business Continuity Plan policy requiring business continuity plan owners whose plan supports a "material" or "significant" rated business process to test their business continuity plans through facilitated exercises (e.g. tabletop exercise, call tree exercise, etc.), maintain evidence of the exercise, and provide documentation to the EBC Team. The EBC Team will update this policy by April 30, 2015 to indicate that such exercises be

conducted at least annually. The EBC Team will also monitor quarterly completion of the exercises and review supporting documentation for adequacy."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSNC provide OPM's HIO evidence of the business continuity policy change and procedures for management review of testing exercises.

b) FEP Business Continuity Plan

We determined that the business continuity policies and procedures specific to BCBSNC's FEP line of business could be improved.

The Plan currently conducts an informal test of the FEP call tree to ensure employees are notified of a disaster. This current process is not defined within policies and no official artifacts are developed in conjunction with the test and the results. NIST 800-34 Revision 1 states "Test results and lessons learned should be documented. . ." Failure to generate testing artifacts increases the risk of inadequate testing and decreases the capacity for oversight of the process.

Recommendation 8

We recommend BCBSNC review and amend the FEP business continuity plan and procedures to include the necessary detail to ensure thorough business continuity tests for the FEP business operations are routinely conducted.

Plan Response to Recommendation 8:

"In response to this recommendation, the Plan agrees. At present, we update our Business Continuity Plan annually and our employee call tree semi annually. To strengthen the procedures we have in place, we will conduct at least one physical test through either a call tree or tabletop exercise per year. Evidence of this exercise will be maintained within the FEP business operations and reported to our Senior Leadership Team (SLT) representative and Enterprise Business Continuity staff. Where appropriate, the results of the exercises will be incorporated into the business continuity plan."

OIG Reply:

As part of the audit resolution process, we recommend that BCBSNC provide OPM's HIO evidence of the FEP business continuity plan testing.

6. Claims Adjudication

The following sections detail our review of the applications and business processes supporting BCBSNC's claims adjudication process. BCBSNC processes all FEP claims through the BCBSA's nationwide FEP Direct claims adjudication system.

a) Application Configuration Management

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

BCBSNC 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:

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

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

b) Claims Processing System

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

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

Nothing came to our attention to indicate that BCBSNC has not implemented adequate controls over the claims processing system.

c) Debarment

BCBSNC has adequate procedures for updating its claims system with debarred provider information. BCBSNC receives the OPM OIG debarment list every month and makes the appropriate updates to the FEP Direct claims processing system. Any claim submitted for a debarred provider is flagged by BCBSNC to adjudicate through the OPM OIG debarment process to include initial notification, a 15 day grace period, and then denial.

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

IV. MAJOR CONTRIBUTORS TO THIS REPORT

INFORMATION SYSTEMS AUDIT GROUP

[redacted], Lead IT Auditor in Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

APPENDIX

February 9, 2015 (Revised: May 18, 2015)

BlueCross BlueShield Association

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.626.4800

[redacted], Group Chief
Claims & IT Audits Group
U.S. Office of Personnel Management
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT AUDIT REPORT
Blue Cross Blue Shield North Carolina IT Audit
Plan Code 310
Report Number 1A-10-33-14-062
(Dated December 9, 2014 and received December 9, 2014)

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

1. Security Management - No Recommendations

2. Access Controls

a. Access to BCBSNC Facilities:

Recommendation 1

We recommend that BCBSNC conduct a review of its physical access controls and implement some form of [redacted] prevention controls at its facilities entrances.

Plan Response

In response to this recommendation, we have determined that the existing physical access controls are appropriate to minimize the likelihood of [redacted]. Currently, the plan has the following controls in place to enforce the physical access of our buildings: electronic security technology, on-site security personnel, badge readers, CCTV cameras, restricted access to restricted areas, security and safety policies and procedures, door alarms etc.

b. Physical Access Recertification:

Recommendation 2

We recommend that BCBSNC implement a process for routinely auditing all active access cards to ensure that they are not assigned to terminated employees; this process should include written confirmation from managers.

Plan Response

In response to this recommendation, The Plan agrees to investigate and improve its current process and remediate, as appropriate, second quarter, June 30, 2015.

3. Network Security

a. Vulnerabilities Noted in Automated Scans:

System Patching

Recommendation 3

We recommend that BCBSNC implement procedures and controls to ensure that [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis**.**

Plan Response

BCBSNC Security Management meets with the Security Operations team weekly and monthly providing monitoring and oversight to ensure that the existing policies and procedures are being followed. Vulnerabilities are assessed for risk, assigned remediation timelines, and remediated according to the guidelines in the documented procedures. Application supportability and availability are factors that determine and possibly dictate timelines for deployment of patches, service packs, and hot fixes. In instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as [redacted], [redacted], [redacted] [redacted] and [redacted]. The Plan will utilize continuous improvement for all items related to securing our [redacted]

[redacted]. In addition, the Plan will continue to review and, if appropriate, update the established policies and procedures to ensure [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis or compensating controls are identified for significant risk items.

Recommendation 4

We recommend that BCBSNC implement procedures and controls to ensure that [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis.

Plan Response

BCBSNC Security Management meets with the Security Operations team weekly and monthly providing monitoring and oversight to ensure that the existing policies and procedures are being followed. Vulnerabilities are assessed for risk, assigned remediation timelines, and remediated according to the guidelines in the documented procedures. Application supportability and availability are factors that determine and possibly dictate timelines for deployment of patches, service packs, and hot fixes. In instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as [redacted], [redacted], [redacted] [redacted] and [redacted]. The Plan will utilize continuous improvement for all items related to securing our [redacted] [redacted]. In addition, the Plan will continue to review and, if appropriate, update the established policies and procedures to ensure [redacted] are installed with appropriate patches, service packs, and hotfixes on a timely basis or compensating controls are identified for significant risk items.

b. Noncurrent Software:

Recommendation 5

We recommend that BCBSNC implement a methodology to ensure that only current and supported versions of system software are installed on [redacted].

Plan Response

BCBSNC is aware that some unsupported software runs on our network and agree it would be preferable for all software to be at current versions. There will be occasions where the Plan's business and Information Technology Group (ITG) departments partner to make risk-aware decisions to not upgrade or replace software. Software that is to become unsupported is inventoried and the impacts of upgrading, replacing, or accepting risk are discussed with business owners. Decisions to not upgrade low risk software may be based on business drivers such as 'Reliant applications are to be retired' or 'the Plan will pay for extended vendor support until internal resources are available for the upgrade'. In instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as Network Intrusion Prevention, Firewalls, Network Access Controls and advanced malware detection tools.

The Plan has a Technology Roadmap in place to address software and hardware currency. With this plan, unsupported software may be needed while ramping up the current software and hardware. For any unsupported software in place during the audit, compensating controls and alternate methods to mitigate any risks were in place and continue to be monitored. The Plan continues to look for methods to improve all items related to securing our [redacted]

Recommendation 6

We recommend that BCBSNC implement a methodology to ensure that only current and supported versions of system software are installed on the user [redacted]

Plan Response

BCBSNC is aware that some unsupported software runs on the [redacted] and agree it would be preferable for all software to be at current versions. There will be occasions where the Plan's business and Information Technology Group (ITG) departments partner to make risk-aware decisions to not upgrade or replace software. Software that is to become unsupported is inventoried and the impacts of upgrading, replacing, or accepting risk are discussed with business owners. Decisions to not upgrade low risk software may be based on business drivers such as 'Reliant applications are to be retired' or 'the Plan will pay for extended vendor support until internal resources are available for the upgrade'. In instances where legacy software is needed to support BCBSNC business applications or patching would negatively impact a BCBSNC business application, BCBSNC may seek alternate methods to mitigate the risk by leveraging third party security tools such as Network Intrusion Prevention, Firewalls, Network Access Controls and advanced malware detection tools.

The Plan has a Technology Roadmap in place to address software and hardware currency. With this plan, unsupported software may be needed while ramping up the current software and hardware. For any unsupported software in place during the audit, compensating controls and alternate methods to mitigate any risks were in place and continue to be monitored. The Plan continues to look for methods to improve all items related to securing our [redacted]

4. Configuration Management – No Recommendations

5. Contingency Planning

a. Business Continuity Plan Tests:

Recommendation 7

We recommend BCBSNC document the business continuity tests results and implement a process for managerial review.

Plan Response

In response to this recommendation, the Plan agrees.

FEP business operations will conduct at least one physical test through either a call tree or tabletop exercise per year. Evidence of this exercise will be maintained within the FEP business operations area and reported to its Senior Leadership Team (SLT) representative and the Enterprise Business Continuity (EBC) Team.

Effective immediately, the Enterprise Business Continuity (EBC) Team will reinforce its current Business Continuity Plan policy requiring business continuity plan owners whose plan supports a “material” or “significant” rated business process to test their business continuity plans through facilitated exercises (e.g. tabletop exercise, call tree exercise, etc.), maintain evidence of the exercise, and provide documentation to the EBC Team. The EBC Team will update this policy by **April 30, 2015** to indicate that such exercises be conducted at least annually. The EBC Team will also monitor quarterly completion of the exercises and review supporting documentation for adequacy.

b. FEP Business Continuity Plan:

Recommendation 8

We recommend BCBSNC review and amend the FEP business continuity plan and procedures to include the necessary detail to ensure thorough business continuity tests for the FEP business operations are routinely conducted.

Plan Response

In response to this recommendation, the Plan agrees. At present, we update our Business Continuity Plan annually and our employee call tree semi-annually. To strengthen the procedures we have in place, we will conduct at least one physical test through either a call tree or tabletop exercise per year. Evidence of this exercise will be maintained within the FEP business operations and reported to our Senior Leadership Team (SLT) representative and Enterprise Business Continuity staff. Where appropriate, the results of the exercises will be incorporated into the business continuity plan.

6. Claims Adjudication – No Recommendations

7. Health Insurance Portability and Accountability Act – No Recommendations

Thank you for the opportunity to provide a response to the Draft Report. If you have any questions in the interim, please contact [redacted] at [redacted]@bcbsa.com or at [redacted].

Sincerely,

[redacted], CISA
Managing Director, FEP Program Assurance

cc: [redacted], BCBSNC
[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

-- CAUTION --

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