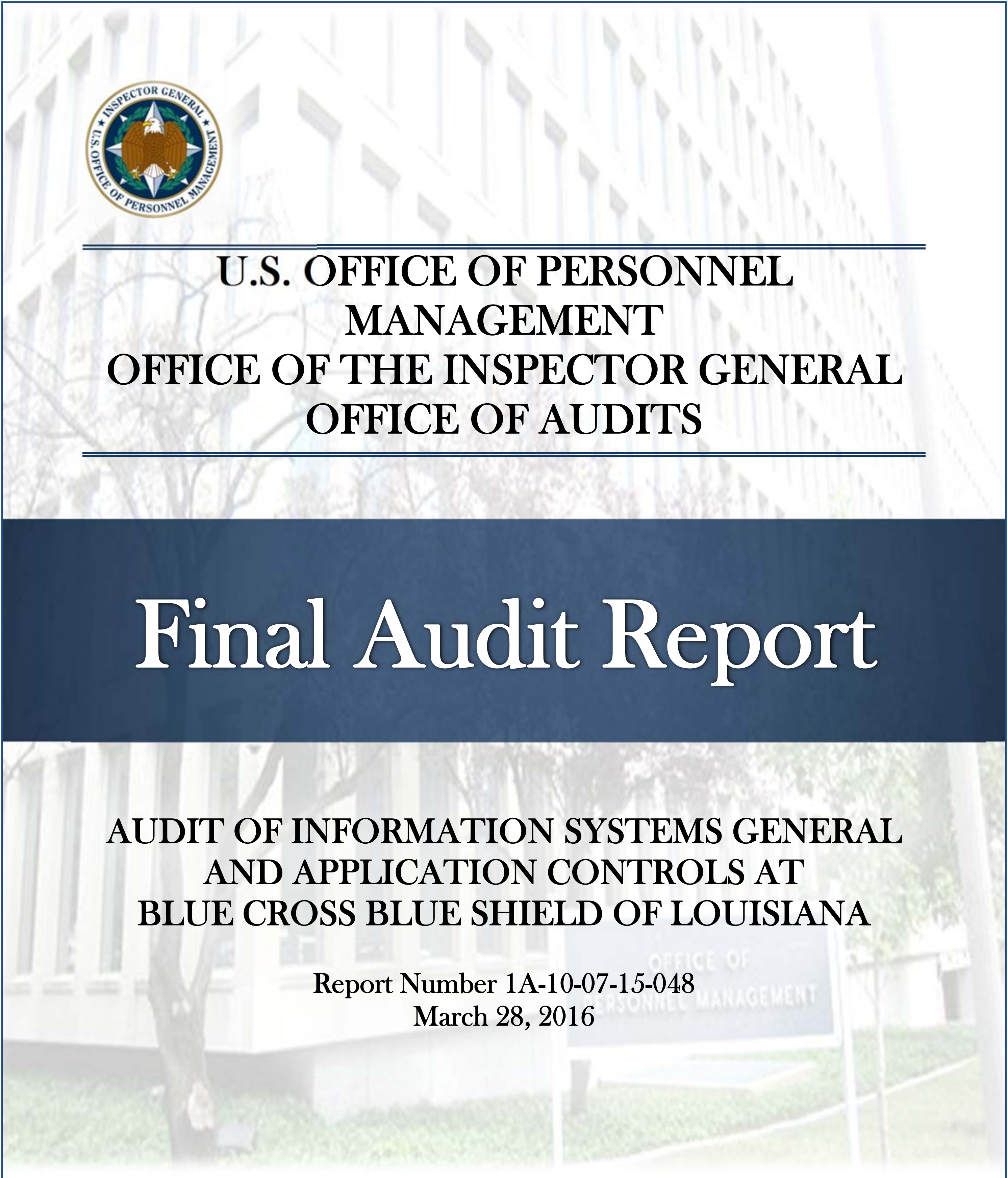

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

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

Report Number 1A-10-07-15-048
March 28, 2016

-- 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 Louisiana

Report No 1A-10-07-15-048 **March 28, 2016**

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

Why Did We Conduct the Audit?
The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in BCBSLA's information technology (IT) environment.

What Did We Audit?
The scope of this audit centered on the information systems used by BCBSLA to process and store data related to medical encounters and insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?
Our audit of the IT security controls of BCBSLA determined that:

- BCBSLA has established an adequate security management program.
- BCBSLA has implemented a variety of 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 BCBSLA's access controls:
  - Several information systems did not require complex passwords in accordance with corporate policy.
  - Multi-factor authentication is not required for privileged user authentication.
  - The process for assigning physical access badges could be improved.
- BCBSLA has implemented an incident response and network security program. However, we noted several areas of concern related to BCBSLA's network security controls:
  - BCBSLA performs routine vulnerability scans; however, the Plan does not always use credentials adequate to perform a thorough test.
  - A patch management policy is in place, but our test work indicated that all patches are not always implemented in a timely manner.
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized.
- BCBSLA has developed formal configuration management policies and has approved baseline configurations for its operating platforms. However, the Plan does not maintain a single inventory of all the network devices, servers, and databases in its technical environment.
- BCBSLA's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. The Plan 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.
- BCBSLA has implemented many controls in its claims adjudication processes to ensure that FEHBP claims are processed accurately. However, we noted several opportunities for improvement in BCBSLA's claims application controls.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
BCBSA	**Blue Cross Blue Shield Association**
BCBSLA	**Blue Cross Blue Shield of Louisiana**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Systems Control Audit Manual**
GAO	**U.S. Government Accountability Office**
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 Louisiana**

TABLE OF CONTENTS

Page

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 Louisiana (BCBSLA 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.

All BCBSLA personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

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

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in BCBSLA'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; and
- Application controls specific to BCBSLA's claims processing systems.

Scope

BCBSLA has a nationwide fee-for-service plan sponsored by the Blue Cross and Blue Shield Association's (BCBSA) Federal Employee Program (FEP).

The scope of this audit centered on the information systems used by BCBSLA to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. BCBSLA processes FEP claims through a local claims processing system that it maintains and also through FEP Direct, the BCBSA nation-wide claims adjudication system. The business processes reviewed are primarily located in BCBSLA's Baton Rouge, Louisiana facilities.

The on-site portion of this audit was performed in June and July of 2015. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSLA as of August 2015.

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

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 BCBSLA'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 BCBSLA'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.

In conducting this review we:

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

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, An Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

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

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

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

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

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

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

B. Access Controls

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

We examined the physical access controls of BCBSLA's facilities and data centers located in Baton Rouge, Louisiana. We also examined the logical controls protecting sensitive data in BCBSLA'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;
- Routinely auditing user access; and
- Adequate environmental controls over the data center.

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

1. Authentication Standards

BCBSLA has documented corporate authentication standards. However, we identified instances where information systems did not enforce complex passwords and were not configured in compliance with the corporate standards.

The "Access Controls" section of FISCAM provides guidance for implementing strong authentication controls. Failure to enforce strong authentication requirements on information systems increases the risk that the systems could be breached by brute force password attacks.

Recommendation 1

We recommend that BCBSLA make the appropriate system changes to ensure that all systems require complex passwords that comply with the corporate authentication policy.

BCBSLA Response:

"The Plan agrees with the recommendation. Implementation of complex passwords on remaining systems was completed on November 3, 2015. See Attachment 1 to support that the recommendation was implemented."

OIG Comment:

In response to our draft audit report, BCBSLA provided a screenshot indicating that it has configured its default Windows domain policy to require complex passwords that comply with the corporate authentication policy. However, during the fieldwork phase of this audit (June 2015) we saw similar evidence that also seemed to indicate that domain passwords were configured to enforce complex passwords. The issue is that our test work determined that this policy was not being adequately enforced on a variety of specific servers in the technical environment. We do not consider the evidence provided in response to the draft report to be sufficient proof that the recommendation has been remediated, as it is the same evidence that was provided to us in in June 2015 when we determined that the controls were not working properly.

2. Privileged User Authentication

Access to privileged user (system administrator) accounts require the use of a password management tool for temporary privilege elevation; administrators must first authenticate to the tool before being granted privileged credentials. Although this control adds security value, we also expect all FEHBP contractors to have multifactor authentication for administrator-level access to information systems. BCBSLA is actively pursuing solutions to implement multifactor authentication for system administrators, however, the control had not been implemented during our fieldwork.

The Federal government requires multi-factor authentication for all information system users. Although BCBSLA is not a government entity, it does process sensitive healthcare data on Federal employees. Therefore, we are recommending that BCBSLA implement this control for privileged users at a minimum. NIST 800-53, Revision 4, states that information systems should implement multifactor authentication for network access to privileged accounts. Failure to implement multifactor authentication increases the risk that privileged user credentials could be compromised and that unauthorized users could access sensitive and proprietary data.

Recommendation 2

We recommend that BCBSLA require multifactor authentication for privileged user access to information systems.

BCBSLA Response:

"The Plan agrees with the recommendation. Multifactor authentication is in the process of being implemented with anticipated role [sic] out to privileged users for first quarter of 2016."

OIG Comment:

As part of the audit resolution process, we recommend that BCBSLA provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this report that BCBSLA agrees to implement.

3. Physical Access Badges

We were told that BCBSLA assigns each employee and contractor a unique identification (ID) badge. During testing, we identified five employees that were assigned multiple ID badges. We also identified 106 active badges that were not assigned to a specific individual.

In response to our testing, BCBSLA stated that all unassigned badges were in its physical possession and that it deactivated the duplicate badges to ensure that employees were no longer assigned more than one. The Plan also stated that it made policy changes to ensure that badge IDs are unique to an individual and that no one has more than one badge. NIST 800-53, Revision 4, states that the organization maintains a list of authorized individuals that are allowed access to the facility. It also says that the organization should review the access list and remove access appropriately.

Failure to maintain adequate controls over physical access badges increases the risk that individuals could gain unauthorized entry to BCBSLA facilities and access sensitive or proprietary information.

Recommendation 3

We recommend that BCBSLA implement a process to routinely audit active badges to ensure that no individual has more than one badge, and that all active badges are assigned to an individual.

BCBSLA Response:

"The Plans [sic] agrees with the recommendation. Current policy was updated to reflect the recommendation and the first routine audit is scheduled for first quarter of 2016. See Attachment 2 to support that the recommendation was implemented."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that BCBSLA has updated its policy/procedures related to physical access badges. The new policy requires a quarterly reconciliation of the active employee badge roster to a separated/terminated list of all ID badges that were deactivated in accordance with Human Resources notifications. As part of the audit resolution process, we recommend that BCBSLA provide OPM's HIO with evidence that it has performed a quarterly reconciliation.

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 BCBSLA's network security program and reviewed the results of automated vulnerability scans performed by the Plan during this audit. We noted the following opportunities for improvement related to BCBSLA's network security controls.

1. Credentialed Vulnerability Scanning

BCBSLA has not historically used adequate system privileges when conducting vulnerability scans.

We conducted a review of BCBSLA's computer server vulnerability management program to determine if adequate controls were in place to detect, track, and remediate vulnerabilities.

BCBSLA performs routine automated scans on its network environment to detect vulnerabilities. However, our review of historical scan reports indicated that BCBSLA has not been effective in ensuring that all systems are scanned regularly, that the scans are performed with system privileges adequate to conduct a thorough review, and that the scanning tools are successfully authenticating to all devices and servers scanned.

The Plan has already taken steps to improve its vulnerability management process and has recently transitioned to a different primary scanning tool. The scan results we reviewed show an increase in the number of servers being adequately scanned during this transition period.

NIST SP 800-53, Revision 4, states that the organization should implement privileged access authorization for vulnerability scanning activities. "Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning."

Failure to perform privileged vulnerability scanning increases the risk that system flaws go undetected, leaving the Plan exposed to unknown threats.

Recommendation 4

We recommend that BCBSLA implement new procedures to ensure that all computer servers and network devices are routinely subject to a vulnerability scan with credentials adequate to perform a thorough test.

BCBSLA Response:

"The Plan agrees with the recommendation. New procedures were implemented in the fourth quarter of 2015 to include scanning of all servers and network devices on a rolling basis and to include implementing privileged access authorization for scanning activities. See Attachment 3 to support that the recommendation was implemented."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that BCBSLA has implemented new procedures to routinely scan all computer servers and network devices with privileged access authorization; no further action is required.

2. Vulnerabilities Identified in Automated Scans

As part of this audit we also asked BCBSLA to perform vulnerability scans on a sample of servers, databases, and user workstations under our supervision using scanning policies that we configured. This test work identified a variety of vulnerabilities that could have been previously detected and remediated by BCBSLA if it had a more mature vulnerability management program in place. The specific vulnerabilities that we identified will not be detailed in this report, but are summarized at a high level below.

System Patching

BCBSLA has documented patch management policies and procedures. [redacted] The missing patches include both operating system and third-party software.

Noncurrent software

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

Secure Configuration Vulnerabilities

The results of the scans also detected isolated instances of server configuration vulnerabilities with known exploits.

Database Vulnerabilities

The results of the database vulnerability scans also indicated that BCBSLA databases have several vulnerabilities that are susceptible to common malicious attack methods.

FISCAM states that "software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, states that the Plan must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly. FISCAM also states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Recommendation 5

We recommend that BCBSLA update its patch management procedures to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.

BCBSLA Response:

"The Plan agrees with the recommendation. Updated patch management procedures will be implemented in the first quarter of 2016 to ensure production server operating systems are updated with the appropriate patches, service packs and hotfixes."

Recommendation 6

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

BCBSLA Response:

"The Plan agrees with the recommendation. While current oversight does exist, a formal methodology is needed to ensure that only supported operating systems are installed on production servers and workstations. This will be implemented in the first quarter of 2016."

Recommendation 7

We recommend that BCBSLA make the appropriate changes to it servers, workstations, and databases to address the specific vulnerabilities identified in our vulnerability scans.

BCBSLA Response:

"The Plan agrees with the recommendation. This will be implemented in the second quarter of 2016."

D. Configuration Management

Configuration management consists of the policies and procedures used to ensure systems are configured according to approved risk-based configuration controls.

The BCBSLA claims processing system is supported by multiple applications in a server environment composed of Windows and UNIX systems. These systems are predominantly running in a virtual environment. Servers are created from standard virtual images and configured according to the intended role. Each server is routinely scanned for compliance with configuration templates built into the virtual management software.

We reviewed the BCBSLA configuration management program and observed the following controls in place:

- Standard configuration baselines;
- Thorough change management process; and
- Routine configuration compliance scanning.

However, we did identify one needed area of improvement related to inventory management. BCBSLA does not maintain a centralized inventory of all network devices, servers, and databases. The plan currently uses multiple tools that are managed by different departments to track systems and network devices. The inventory documentation we reviewed did not appear to be complete or consistent between the various sources. BCBSLA has identified this as an area for improvement and is exploring options for creating a comprehensive device inventory. However, the control had not been implemented during our fieldwork.

We expect to see device inventory that is centrally maintained and supported at a high level in the organization. The inventory should serve as an authoritative record and facilitate multiple areas of information security governance. Elements of a security program that depend on an accurate inventory include configuration management, patch management, and security vulnerability testing.

FISCAM states that “To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their systems. Without one, the entity cannot effectively manage IS controls across the entity.”

Failure to maintain a complete inventory increases the risk that devices are omitted from security processes and continue to reside on the network with significant security vulnerabilities.

Recommendation 8

We recommend that BCBSLA develop and maintain a single comprehensive inventory of all the network devices, servers, and databases in its technical environment.

BCBSLA Response:

"The Plan agrees with the recommendation. Inventory Management, to include hardware, as part of IT Asset Management will be completed by third quarter 2016. The Configuration Management Database (CMDB) will include servers, network equipment and databases by end of third quarter 2016."

E. Contingency Planning

BCBSLA has adequate controls over its contingency planning process.

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

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

We determined that the service continuity documentation contained the critical elements suggested by NIST SP 800-34, Revision 1. BCBSLA 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.

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

F. Application Controls

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

1. Application Configuration Management

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

BCBSLA has documented system development life cycle procedures that IT personnel follow during routine software modifications. All changes require approval and undergo testing prior to migration to the production environment. We do not have any concerns regarding BCBSLA's application configuration management process.

2. Claims Processing System

We evaluated the input, processing, and output controls associated with the BCBSLA claims processing systems. We determined that BCBSLA 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 BCBSLA has not implemented adequate controls over its claims processing systems.

3. Debarment

BCBSLA has adequate procedures for updating its claims system with debarred provider information. BCBSLA receives the OPM OIG debarment list every month and compares it to the BCBSLA provider database and claims processing system. If a match is found, the systems are updated appropriately. Any claim submitted for a debarred provider is flagged by BCBSLA 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 BCBSLA has not implemented adequate controls over the debarment process.

4. Application Controls Testing

We conducted a test on BCBSLA'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 BCBSLA's system adjudicated the claims. All claims are first processed in the BCBSLA local claims processing system and then routed to the BCBSA's nationwide claims processing system called FEP Direct.

Our test results indicated that BCBSLA's system has controls and system edits in place to identify many of our test scenarios.

The sections below document opportunities for improvement related to BCBSLA's claims application controls.

i. Medical Editing

Our claims testing exercise identified several scenarios where BCBSLA's claims processing system and FEP Direct failed to detect medical inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- *Diagnosis / Procedure (Professional)* – (1) a procedure code for a spinal manipulation with a diagnosis of a heart attack; (2) a procedure code for brain surgery with a diagnosis of abdominal pain; and (3) a procedure code for a toe amputation and a diagnosis of a headache;
- *Age / Procedure (Professional & Facility)* – (1) a procedure code for an intrauterine device insertion with a 9-year-old female patient; (2) a 10-year-old female patient giving birth; and (3) a 98-year-old female giving birth;
- *Invalid Place of Service (Professional)* – (1) a procedure code for a heart surgery with a place of service code for residential substance abuse facility; and (2) a procedure code for a brain surgery with a place of service code for a residential abuse facility; and
- *Provider / Procedure Inconsistencies (Professional)* – (1) claims were processed and paid to a chiropractor that performed heart surgery, shoulder surgery, and brain surgery; (2) claims were processed and paid to a nurse practitioner that performed heart surgery, shoulder surgery, and brain surgery.

Failure to detect these medical inconsistencies increases the risk that benefits are being paid for procedures that were not actually paid.

The BCBSA has an ongoing project in place related to improving the medical edits within FEP Direct. The specific scenarios identified in this audit should be analyzed as part of that project.

<u>Recommendation 9</u>

We recommend that the BCBSA review the scenarios documented above related to medical edits and ensure that they are analyzed as part of the FEP Direct medical edits project.

<u>BCBSA Response:</u>

"BCBSA evaluated FEP claims payment history for all of the scenarios listed in the recommendation for the period of January 2014 thru September 2015 and did not identify any actual claim payments to providers for the scenarios listed.

BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, [2016] to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received."

ii. Patient History

Our claims testing exercise identified several scenarios where BCBSLA's claims processing system and FEP Direct failed to detect patient history. For each of the following scenarios, a test claim was incorrectly processed without encountering any edits.

- *Near Duplicate Claims (Professional)* – (1) a test claim with a brain surgery procedure code was submitted, then processed and paid appropriately. Another claim was submitted with the same brain surgery procedure code, same patient, same date of service, but with a different provider that also processed and paid; (2) a test claim with a shoulder surgery procedure code was submitted, then processed and paid appropriately. Another claim was submitted with the same shoulder surgery procedure code, same patient, same date of service, but with a different provider that also processed and paid; and
- *Once Per Lifetime Procedures (Facility)* – (1) a test claim was submitted for a woman that gave birth and was processed and paid appropriately. Another test claim was submitted with a date of service a month later for the same woman giving birth and the claim processed and paid; (2) a test claim was submitted for a woman that had a hysterectomy and was processed and paid appropriately. A subsequent test claim was submitted for the same woman having another hysterectomy two months later.

Failure to detect these patient history issues increases the risk that benefits are being paid for procedures that were not actually performed.

We identified issues with the way in which FEP Direct analyzes a patient's history as part of an audit of another BCBS plan (Report No. 1A-10-49-14-021). The specific scenarios identified in this audit should be analyzed as part of the efforts to address that existing recommendation.

Recommendation 10

We recommend that the BCBSA review the scenarios documented above related to patient history and ensure that they are analyzed as part of the ongoing efforts to address patient history edits in FEP Direct.

BCBSA Response:

"A near duplicate deferral was implemented in the FEP claims system on September 27, 2015 that will address the near duplicate scenarios identified. See Attachment 4 for examples of claims tested after the system enhancement and Attachment 5 for current system documentation on the new near duplicate deferral.

For the patient history inconsistencies, BCBSA evaluated FEP claims payment history for all of the scenarios listed in the recommendation for the period of January 2014 thru September 2015 and did not identify any actual claim payments to providers for the scenarios listed.

BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, [2016] to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that BCBSA has implemented a deferral in FEP Direct; no further action is required related to the "near-duplicate claims" inconsistency. We recommend that BCBSA provide OPM's HIO with evidence that the patient history inconsistency related to "once in a lifetime procedures" has been implemented.

iii. Modifiers

Our claims testing exercise identified several scenarios where BCBSLA's claims processing system and FEP Direct failed to detect claims that contained inappropriately used procedure code modifiers. For each of the following scenarios, a test claim was incorrectly processed without encountering any edits detecting the inconsistency.

- *Modifiers 22, 59, 62, 66 (Professional)* - (1) a test claim with a procedure code for a brain surgery with a modifier 22 processed and paid without pending. The American Medical Association (AMA) requires supporting documentation to be provided when modifier 22 is used; (2) a test claim with a procedure code for an evaluation and management service was submitted with a modifier 59 that processed and paid without pending. The AMA also requires supporting documentation to be provided when this modifier is used; (3) a team surgery claim with a modifier 66 processed and paid for a procedure that doesn't allow team surgery; and (4) a co-surgeon claim with modifier 62 was processed and paid for a procedure that does not allow co-surgery.

Failure to detect these modifier issues increases the risk that benefits are being inappropriately paid.

Recommendation 11

We recommend that the BCBSA review the scenarios documented above related to modifiers and ensure that the appropriate system edits are implemented in FEP Direct. BCBSA should determine which specific BCBS plans increase payments for modifier 22, and ensure that FEP Direct can appropriately defer modifier 22 claims for these plans.

BCBSA Response:

Modifier 22

BCBSA disagrees with this recommendation and stated in its response that the modifier 22 scenario does not apply to BCBSLA because the Louisiana provider plan contracts do not include an increase in payment to the provider when modifier 22 is included with a procedure code. BCBSA also stated that it is not necessary to make a system change in FEP Direct because "Each Plan provider contract is specific on whether or not an additional payment will be made when modifier 22 is used and in many cases use of the modifier does not change the amount paid for the procedure."

OIG Comment:

We have evaluated BCBSA's response and agree that BCBSLA should not be required to implement an edit for the modifier 22 issue because this Plan's provider contracts do not include an increase in payment to the provider when modifier 22 is used. We modified the draft report recommendation to make the final recommendation specific to the nationwide FEP Direct system. We also agree that it may not be appropriate to implement a deferral for all modifier 22 claims on FEP Direct, considering each Plan provider contract is unique regarding whether or not an additional payment will be made when modifier 22 is used. However, many BCBS Plans do pay additional benefits when modifier 22 is used, and the AMA requires additional supporting documentation to be provided with these claims.

Therefore, we updated the recommendation to also recommend that BCBSA determine which specific BCBS plans increase payments for modifier 22, and ensure that FEP Direct can appropriately defer modifier 22 claims for these plans so that the claims evaluators can review the supporting documentation that should come with the claim before approving payment to the provider.

Modifier 59

"BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, [2016] to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received.

Modifiers 62 and 66

"BCBSA implemented a deferral for modifier 62 and 66 in the FEP claims system on September 27, 2015 that will address the recommendation related to modifier 62 and 66 deferral for review. See Attachment 6."

OIG Comment:

Evidence was provided in response to the draft audit report that indicates that BCBSA has implemented a deferral in FEP Direct related to modifiers 62 and 66; no further action is required.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Senior Team Leader

[redacted], Group Chief

APPENDIX

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

January 11, 2016

[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 Louisiana IT Audit
Plan Codes 170/270
Audit Report Number 1A-10-07-15-048
(Dated November 3, 2015)

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

B. Access Controls

1. Authenticated Standards

Recommendation 1

We recommend that BCBSLA make the appropriate system changes to ensure that all systems require complex passwords that comply with the corporate authentication policy.

Plan Response

The Plan agrees with the recommendation. Implementation of complex passwords on remaining systems was completed on November 3, 2015. See Attachment 1 to support that the recommendation was implemented.

2. Privileged User Authentication

Recommendation 2

We recommend that BCBSLA require multifactor authentication for privileged user access to information systems.

Plan Response

The Plan agrees with the recommendation. Multifactor authentication is in the process of being implemented with anticipated role out to privileged users for first quarter of 2016.

3. Physical Access Badges

Recommendation 3

We recommend that BCBSLA implement a process to routinely audit active badges to ensure that no individual has more than one badge, and that all active badges are assigned to an individual.

Plan Response

The Plans agrees with the recommendation. Current policy was updated to reflect the recommendation and the first routine audit is scheduled for first quarter of 2016. See Attachment 2 to support that the recommendation was implemented.

C. Network Security

Redacted by the OIG. This recommendation was removed from the final audit report

[1]. Credentialed Vulnerability Scanning

Recommendation [4]

We recommend that BCBSLA implement new procedures to ensure that all computer servers and network devices are routinely subject to a vulnerability scan with credentials adequate to perform a thorough test.

Plan Response

The Plan agrees with the recommendation. New procedures were implemented in the fourth quarter of 2015 to include scanning of all servers and network devices on a rolling basis and to include implementing privileged access authorization for scanning activities. See Attachment 3 to support that the recommendation was implemented.

[2]. Vulnerabilities Identified in Automated Scans

Recommendation [5]

We recommend that BCBSLA updates its patch management procedures to ensure that production servers are updated with appropriate patches, service packs, and hotfixes on a timely basis.

Plan Response

The Plan agrees with the recommendation. Updated patch management procedures will be implemented in the first quarter of 2016 to ensure production server operating systems are updated with the appropriate patches, service packs and hotfixes.

Recommendation [6]

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

Plan Response

The Plan agrees with the recommendation. While current oversight does exist, a formal methodology is needed to ensure that only supported operating systems are installed on production servers and workstations. This will be implemented in the first quarter of 2016.

Recommendation [7]

We recommend that BCBSLA make the appropriate changes to it servers, workstations, and databases to address the specific vulnerabilities identified in our vulnerability scans.

Plan Response

The Plan agrees with the recommendation. This will be implemented in the second quarter of 2016.

3. Configuration Management

Recommendation [8]

We recommend that BCBSLA develop and maintain a single comprehensive inventory of all the network devices, servers, and databases in its technical environment.

Plan Response

The Plan agrees with the recommendation. Inventory Management, to include hardware, as part of IT Asset Management will be completed by third quarter

2016. The Configuration Management Database (CMDB) will include servers, network equipment and databases by end of third quarter 2016.

4. Claims Adjudication

Recommendation [9]

We recommend that the BCBSA review scenarios documented above related to medical edits and ensure that they are analyzed as part of the FEP Direct medical edits project.

BCBSA Response

BCBSA evaluated FEP claims payment history for all of the scenarios listed in the recommendation for the period of January 2014 thru September 2015 and did not identify any actual claim payments to providers for the scenarios listed.

BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, 2015 to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received.

Recommendation [10]

We recommend that the BCBSA review scenarios documented above related to patient history and ensure that they are analyzed as part of the ongoing efforts to address patient history edits in FEP Direct.

BCBSA Response

A near duplicate deferral was implemented in the FEP claims system on September 27, 2015 that will address the near duplicate scenarios identified. See Attachment 4 for examples of claims tested after the system enhancement and Attachment 5 for current system documentation on the new near duplicate deferral.

For the patient history inconsistencies, BCBSA evaluated FEP claims payment history for all of the scenarios listed in the recommendation for the period of January 2014 thru September 2015 and did not identify any actual claim payments to providers for the scenarios listed.
BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, 2015 to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received.

Recommendation [11]

We recommend that the BCBSA review scenarios documented above related modifiers and ensure that the appropriate system edits are implemented in FEP Direct and/or the BCBSLA local system.

Plan Response

The Plan disagrees that a system enhancement to defer claims for further review is required for modifier 22 claims. At this time, Plan provider contracts do not include an increase in payment to the provider when modifier 22 is included with a procedure code. As a result, at this time, there is no need to stop claims for review for appropriate use of this modifier. The Plans will defer any changes or modifications be directed to the Blue Cross and Blue Shield Association to implement.

BCBSA Response:

Modifier 22

BCBSA disagrees that a system enhancement to defer claims for further review is required for modifier 22 claims when there is no impact on the amount paid when the modifier is added to the procedure code. Each Plan provider contract is specific on whether or not an additional payment will be made when modifier 22 is used and in many cases use of the modifier does not change the amount paid for the procedure. Implementation of a deferral in the FEP claims system to defer all modifier 22 claims would not be appropriate at this time.

Modifier 59

BCBSA will submit a request to the FEP Operations Center (FEPOC) by January 31, 2015 to determine the feasibility of enhancing current existing edits to address the scenarios listed above. BCBSA will further evaluate the FEPOC response once received.

Modifiers 62 and 66

BCBSA implemented a deferral for modifier 62 and 66 in the FEP claims system on September 27, 2015 that will address the recommendation related to modifier 62 and 66 deferral for review. See Attachment 6.

We appreciate the opportunity to provide our response to each of the findings 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], CISA
Managing Director, Program Assurance

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