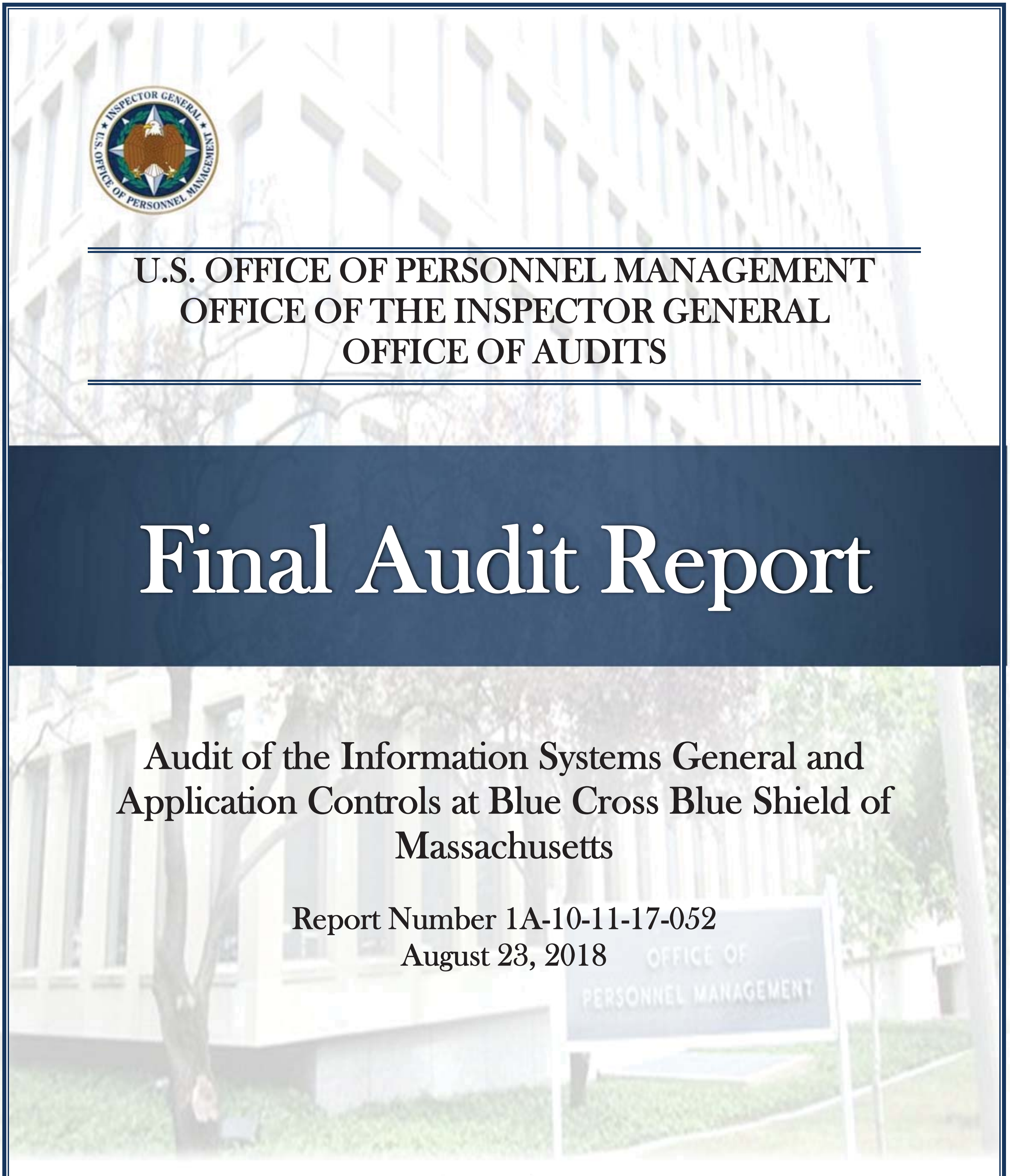

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

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

Report Number 1A-10-11-17-052
August 23, 2018

EXECUTIVE SUMMARY

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

Report No. 1A-10-11-17-052 **August 23, 2018**

Why Did We Conduct the Audit?

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

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

What Did We Audit?

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

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- BCBSMA has established an adequate security management program.

- BCBSMA has adequate physical access controls over its facilities and data centers. However, logical access controls could be improved. [redacted]

- BCBSMA could improve its network security posture by improving [redacted]. Furthermore, BCBSMA does not have controls to prevent [redacted]

- BCBSMA has not documented and approved a formal configuration management policy. Also, BCBSMA has not documented security configuration standards for all of the operating platforms in its network environment. Furthermore, [redacted]

- [redacted]

- BCBSMA has documented contingency plans that are tested on a routine basis.

- BCBSMA has implemented many controls over its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

BCBSA	Blue Cross Blue Shield Association
BCBSMA	Blue Cross Blue Shield of Massachusetts
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FEP	Federal Employee Program
FISCAM	Federal Information System Controls Audit Manual
GAO	U.S. Government Accountability Office
IT	Information Technology
LAN	Local Area Network
NIST SP	National Institute of Standards and Technology’s Special Publication
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management

TABLE OF CONTENTS

I. BACKGROUND

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

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

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

This was our second audit of the information technology (IT) general and application controls at BCBSMA. The previous audit resulted in Report No. 1A-10-11-08-001, dated May 28, 2008. All findings from the previous audit have been closed.

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

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

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

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

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of BCBSMA's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of BCBSMA'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 BCBSMA to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Boston, Massachusetts.

The onsite portion of this audit was performed in October and November of 2017. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSMA as of November 2017.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSMA. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this review we:

- Gathered documentation and conducted interviews;

- Reviewed BCBSMA's business structure and environment;

- Performed a risk assessment of BCBSMA'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 BCBSMA'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;

- 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, Revision 1, An Introduction to Computer Security;

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

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

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

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

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

COMPLIANCE WITH LAWS AND REGULATIONS

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

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

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

BCBSMA has implemented a series of formal policies and procedures that govern its security management program. BCBSMA has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSMA also has implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

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

B. ACCESS CONTROLS

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

We examined the physical access controls at BCBSMA's facilities and datacenters. We also examined the logical access controls protecting sensitive data in BCBSMA's network environment and applications.

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

- Procedures for appropriately granting and removing physical access to facilities and datacenters; and

- Procedures for appropriately granting and adjusting logical access to applications and software resources.

The following section documents an opportunity for improvement related to BCBSMA's logical access controls.

1) [redacted]

[redacted] However, BCBSMA has not completed a review of all [redacted] The organization has informed us that a project has been initiated to review [redacted].

NIST SP 800-53, Revision 4, states that organizations should [redacted] Failure to [redacted] increases the attack surface of information systems.

<u>Recommendation 1</u>

We recommend that BCBSMA complete its review of [redacted]. Furthermore, we recommend that BCBSMA implement an auditing process to ensure that [redacted].

<u>BCBSMA Response:</u>

"BCBSMA agrees with this recommendation.

[redacted]

[redacted]

OIG Comment:

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

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 BCBSMA's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

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

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

1) [redacted]

[redacted]

[redacted]

[redacted] BCBSMA has identified this weakness and has a project in place to remediate the issue.

NIST SP 800-41, Revision 1, advises that, [redacted]

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

Recommendation 2

We recommend that BCBSMA implement security controls [redacted]

BCBSMA Response:

"BCBSMA agrees with this recommendation. BCBSMA has selected a [redacted] ***solution to enhance our technical capabilities. A*** [redacted]***. BCBSMA's*** [redacted] ***will be updated annually to reflect our current*** [redacted] ***controls.*** [redacted]

2) Network Access Control

BCBSMA does not have controls implemented to [redacted] This issue is compounded by [redacted]. However, we were told that BCBSMA has a project in place to install technical tools to address this issue.

NIST SP 800-53, Revision 4, states that [redacted]

<u>Recommendation 3</u>

We recommend that BCBSMA implement [redacted]

<u>BCBSMA Response:</u>

“BCBSMA agrees with this recommendation. BCBSMA has selected a [redacted] ***solution to enhance our technical capabilities.*** [redacted] ***BCBSMA’s*** [redacted] ***will be updated annually to reflect our current*** [redacted]

D. <u>CONFIGURATION MANAGEMENT</u>

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

BCBSMA does not have documented security configuration standards for all operating platforms in use.

- System configuration changes are documented;
- A formal change approval process; and
- An adequate patch management process.

The sections below document areas for improvement related to BCBSMA’s configuration management controls.

1) Configuration Management Policy

BCBSMA’s vulnerability management policy provides high-level guidance related to the secure configuration of systems and applications. However, this policy does not detail many of the elements found in a configuration management policy as described by NIST SP 800-53, Revision 4.

NIST SP 800-53, Revision 4, states that an organization should develop a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, as well as procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Failure to establish an approved configuration management policy increases the risk that systems in the network environment may not be configured in a secure manner.

Recommendation 4

We recommend that BCBSMA document and approve a formal configuration management policy that contains the elements recommended by NIST SP 800-53, Revision 4.

BCBSMA Response:

"BCBSMA agrees with this recommendation. BCBSMA will update its information security policies and related procedures to clarify Configuration Management-related requirements and procedures in accordance with NIST SP 800-53, Revision 4 by June 30, 2018. The updates will reflect key elements included in the NIST guidance for Configuration Management."

2) Security Configuration Standards

BCBSMA configures its servers using a standard image for each operating system. The images are developed internally and maintained by BCBSMA personnel. However, BCBSMA has not established security configuration standards for its systems. Security configuration standards are formally approved documents that detail an organization's approved security settings for each operating system it uses.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system . . . that reflect the most restrictive mode consistent with operational requirements . . . ."

In addition, NIST SP 800-53, Revision 4, also states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved security configuration standards increases the risk that systems may not be configured in a secure manner.

Recommendation 5

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

BCBSMA Response:

"BCBSMA agrees with this recommendation. The security configuration standards have been created. [redacted]

3) Security Configuration Auditing

BCBSMA performs [redacted] audits on its server configurations using an automated tool. However, as noted above, BCBSMA has not documented approved security configuration standards for all operating platforms and databases deployed in its technical environment. Without approved security configuration standards, BCBSMA cannot effectively audit its system's security settings (i.e., there are no approved settings to which to compare the actual settings).

NIST SP 800-53, Revision 4, states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

FISCAM requires current configuration information to be routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system. Failure to perform configuration compliance auditing using approved security configuration standards increases the risk that servers are not configured appropriately, and leaving this undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 6

We recommend that BCBSMA improve its configuration auditing process to routinely audit server configuration settings against an approved configuration standard. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

<u>BCBSMA Response:</u>

"BCBSMA agrees with this recommendation. The security configuration standards have been created. [redacted]

4) System Lifecycle Management

[redacted]

[redacted]

[redacted]

<u>Recommendation 7</u>

[redacted]

<u>BCBSMA Response:</u>

"BCBSMA agrees with this recommendation. [redacted]

[redacted]

E. CONTINGENCY PLANNING

BCBSMA has adequate controls related to contingency planning.

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

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);

- Business continuity plan (e.g., people and business processes);

- Contingency plan tests; and

- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." BCBSMA 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 BCBSMA has not implemented adequate controls related to contingency planning.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSMA's claims adjudication process. BCBSMA prices and adjudicates claims using a vendor-managed claims processing application and the Blue Cross Blue Shield Association's (BCBSA) nationwide Federal Employee Program (FEP) Direct system. We reviewed the following processes related to claims adjudication: application configuration management, claims processing, and provider debarment.

1) Application Configuration Management

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

BCBSMA 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 approval of software modifications:

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

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

2) Claims Processing System

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

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

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

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

3) Debarment

BCBSMA has documented procedures for updating its claims system with debarred provider information. BCBSMA's FEP Compliance & Audits department is notified by BCBSA that an update to the OPM OIG debarment list is available to download. BCBSMA personnel review the list to determine if any debarred providers have active contracts with BCBSMA. If an active provider is determined to be debarred, the provider is flagged in FEP Direct, which will cause any incoming claims to defer for further review. BCBSMA adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

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

APPENDIX

May 2, 2018

BlueCross BlueShield Association

An Association of Independent
Blue Cross and Blue Shield Plans

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

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

Reference: OPM DRAFT IT AUDIT REPORT
Blue Cross Blue Shield of Massachusetts (BCBSMA)
Audit Report Number 1A-10-11-17-052
(Dated March 5, 2018)

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

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

1. [redacted]

Recommendation 1

We recommend that BCBSMA complete its review of [redacted]. Furthermore, we recommend that BCBSMA implement an auditing process to ensure that [redacted]

Plan Response

BCBSMA agrees with this recommendation.

[redacted]

[redacted]

[redacted]

C. NETWORK SECURITY

1. [redacted]

Recommendation 2

We recommend that BCBSMA implement security controls [redacted]

Plan Response

BCBSMA agrees with this recommendation. BCBSMA has selected a [redacted] solution to enhance our technical capabilities. [redacted] BCBSMA's [redacted] will be updated annually to reflect our current [redacted] controls. [redacted]

2. Network Access Control

Recommendation 3

We recommend that BCBSMA implement [redacted]

[redacted]

Plan Response

BCBSMA agrees with this recommendation. BCBSMA has selected a [redacted] solution to enhance our technical capabilities. [redacted] BCBSMA's [redacted] will be updated annually to reflect our current [redacted]

D. CONFIGURATION MANAGEMENT

1. Configuration Management Policy

Recommendation 4

We recommend that BCBSMA document and approve a formal configuration management policy that contains the elements recommended by NIST SP 800-53, Revision 4.

Plan Response

BCBSMA agrees with this recommendation. BCBSMA will update its information security policies and related procedures to clarify Configuration Management-related requirements and procedures in accordance with NIST SP 800-53, Revision 4 by June 30, 2018. The updates will reflect key elements included in the NIST guidance for Configuration Management.

2. Security Configuration Standards

Recommendation 5

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

Plan Response

BCBSMA agrees with this recommendation. The security configuration standards have been created. [redacted]

3. Security Configuration Auditing

Recommendation 6

We recommend that BCBSMA improve its configuration auditing process to routinely audit server configuration settings against an approved configuration standard. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

Plan Response

BCBSMA agrees with this recommendation. The security configuration standards have been created. [redacted]

4. System Lifecycle Management

Recommendation 7

[redacted]

Plan Response

BCBSMA agrees with this recommendation. [redacted]

E. CONTINGENCY PLANNING

No recommendations noted.

F. Claims Adjudication

No recommendation noted.

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

Sincerely,

[redacted]
Managing Director, FEP Program Assurance

cc: [redacted] OPM
[redacted] EP

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