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 MISSISSIPPI

Report Number 1A-10-40-19-010
October 21, 2019

EXECUTIVE SUMMARY

Audit of Information systems General and Application Controls at Blue Cross Blue Shield of Mississippi

Report No. 1A-10-40-19-010 **October 21, 2019**

Why Did We Conduct The Audit?

Blue Cross Blue Shield of Mississippi (BCBSMS) 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 BCBSMS's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSMS 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 BCBSMS's IT security controls determined that:

- BCBSMS has an adequate security management program.
- Formal guidance to prohibit conflicting logical access roles could enhance its segregation of duty procedures.
- BCBSMS does not have a firewall management policy nor does it audit current firewall configurations.
- [redacted].
- Historical vulnerability scans show that sufficient authentication credentials were not used for all systems.
- Our vulnerability scans indicated the presence of vulnerabilities that have not been timely remediated.
- [redacted]. Furthermore, [redacted]
- Due to a change in BCBSMS's backup vendor during audit fieldwork, BCBSMS has not updated or tested its disaster recovery plan since switching primary data center vendors.
- Adequate controls have been implemented to protect sensitive data throughout the claims adjudication process.
- Systems development lifecycle policies and procedures should be updated to require [redacted]

ABBREVIATIONS

BCBSMS	**Blue Cross Blue Shield of Mississippi**
BIA	**Business Impact Analysis**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employees Program**
FISCAM	**Federal Information Systems Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
SDLC	**System Development Life Cycle**

TABLE OF CONTENTS

APPENDIX: BCBSMS August 26, 2019, response to the draft audit report, issued June 5, 2019.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

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 Mississippi (BCBSMS)

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, or comprehensive medical services.

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

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to BCBSMS'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 BCBSMS'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 BCBSMS'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 BCBSMS to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Flowood, Mississippi.

The onsite portion of this audit was performed in January and February of 2019. 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 BCBSMS as of March 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSMS. 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 BCBSMS's business structure and environment;
- Performed a risk assessment of BCBSMS'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 BCBSMS'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;
- Control Objectives for Information and Related Technologies 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-44, Version 2, Guidelines on Securing Public Web Servers;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether BCBSMS's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, BCBSMS 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 BCBSMS's overall IT security program. We evaluated BCBSMS's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSMS has developed an adequate risk management program.

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

Nothing came to our attention to indicate that BCBSMS 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 BCBSMS's facilities and data center. We also examined the logical access controls protecting sensitive data in BCBSMS's network environment and claims processing applications.

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

- Procedures for appropriately managing logical and physical access to health plan facilities, the data center, and information systems;
- Multifactor authentication for privileged user remote access; and
- Routine reviews of logical access to critical information systems.

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

1. Segregation of Duties

Business area managers are responsible for designating access rights to all information systems and applications for new employees. However, [redacted]

FISCAM states that "Entity-wide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced."

[redacted]

Recommendation 1

We recommend that BCBSMS [redacted]

BCBSMS's Response:

"BCBSMS agrees with this recommendation. [redacted] ***The target implementation date is November 30, 2019."***

OIG Comments:

As a part of the audit resolution process, we recommend that BCBSMS provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement also applies to subsequent recommendations in this audit report that BCBSMS 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 the BCBSMS network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Network access controls to prevent unauthorized devices on the internal network; and
- Documented policies and procedures to identify and respond to information security incidents.

However, we noted the following opportunities for improvement related to BCBSMS's network security controls.

1. Documented Firewall Management Policy

BCBSMS has a process to configure and control changes to firewall devices on its network using a deny all approach. However, the Plan has not documented this process in a formal policy or procedure to define the requirements.

BCBSMS does not have a formally documented firewall management policy.

During our audit, BCBSMS created a draft firewall policy, but the policy has not been formally reviewed or approved. The document also does not contain some of the key elements or details recommended by NIST SP 800-41, Revision 1, including:

- "[H]ow firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies";
- Guidance on performing risk assessments to create a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances; and
- Specific guidance on how to address changes to the ruleset including a log of all policy decisions and ruleset changes.

NIST SP 800-41, Revision 1, also states that a firewall policy should be documented and updated frequently.

Failure to develop and maintain a detailed firewall policy could lead to improper management of critical network connections.

Recommendation 2

We recommend that BCBSMS develop and maintain a detailed firewall management policy to provide guidance for [redacted] firewalls as well as approving and documenting changes.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. [redacted] ***This was completed July 31, 2019."***

2. Firewall Configuration Review

As previously stated, BCBSMS does not have a formal documented firewall management policy. [redacted].

NIST SP 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that the firewall rules are in compliance with the organization's policies.

Failure to routinely audit firewall settings increases the risk that unauthorized changes to the firewall's configuration remain undetected.

Recommendation 3

We recommend that BCBSMS perform routine audits of its current firewall configurations against an approved firewall policy. Note – this recommendation cannot be implemented until the controls from Recommendation 2 are in place.

BCBSMS's Response:

"BCBSMS agrees with this recommendation [redacted] ***This was completed July 31, 2019."***

3. [redacted]

BCBSMS uses [redacted] BCBSMS has initiated a project to [redacted] in the near future.

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

Failure to [redacted] increases the risk [redacted]

Recommendation 4

We recommend that BCBSMS [redacted]

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS will continue to work on completing the [redacted] ***The target implementation date is December 31, 2020."***

4. Vulnerability Scanning

BCBSMS stated that their information security team performs [redacted] vulnerability scans on all systems in its network environment. The Plan also stated that all scans are conducted with full administrative privileges. However, we requested evidence and several scans indicated that the accounts used for the vulnerability scans did not provide adequate access to several systems being tested.

NIST SP 800-53, Revision 4, states, "The information system implements 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."

Several historical vulnerability scans did not use adequate authentication credentials.

Failure to maintain a comprehensive internal vulnerability scanning program increases the risk that system flaws would not be identified, leaving BCBSMS susceptible to attacks.

Recommendation 5

We recommend that BCBSMS ensure the [redacted] vulnerability scans are conducted with sufficient access to perform a thorough scan.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS will work to ensure that adequate access to all systems, where applicable, is in place to perform thorough vulnerability scans. If full credentialed scans cannot be performed, a risk assessment will be conducted. The target implementation date is October 31, 2019."

5. OIG Vulnerability Scanning

We conducted credentialed vulnerability and configuration compliance scans on a sample of servers in BCBSMS's network environment. The specific vulnerabilities that we identified were provided to BCBSMS in the form of an audit inquiry, but will not be detailed in this report. The Plan stated that they are analyzing the risk for each of the identified issues and will take appropriate actions once the analysis is complete.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 6

We recommend that BCBSMS remediate the specific [redacted] discovered during this audit as outlined in the vulnerability scan audit inquiry.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS will work to have all identified [redacted] ***remediated. The target implementation date is September 30, 2019."***

D. CONFIGURATION MANAGEMENT

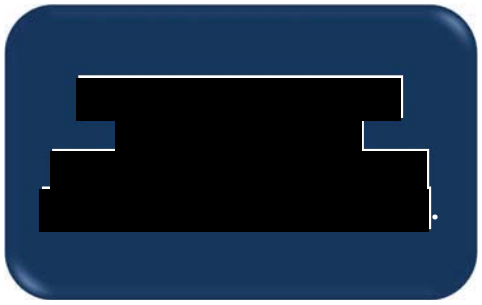
Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. BCBSMS employs a team of technical personnel who manage system software configuration for the organization. We evaluated BCBSMS's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented system change control process; and
- Established patch management process.

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

1. Security Configuration Standards



BCBSMS has documented policies that require the implementation of a baseline hardening procedure. BCBSMS follows a standard build process to install and setup new servers. BCBSMS has also begun implementation of a security configuration baseline for one of the operating systems in its network environment. However, implementation of the [redacted] for the other operating systems in the BCBSMS environment. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

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

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

[redacted]

Recommendation 7

We recommend that BCBSMS [redacted].

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS will work to [redacted] ***The target implementation date is October 31, 2019."***

2. Security Configuration Auditing

As noted above, BCBSMS [redacted]

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.

[redacted].

Recommendation 8

We recommend that BCBSMS implement a process to [redacted] Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. [redacted] ***The target implementation date is November 30, 2019."***

E. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of BCBSMS's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to BCBSMS 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);
- Disaster recovery plan tests; and
- Emergency response procedures.

The section below documents areas for improvement related to BCBSMS's contingency planning controls.

1. Disaster Recovery Plan and Testing

BCBSMS outsources its back-up data center operations to a third party and performs a functional disaster recovery test every year. In 2018, the Plan entered into an agreement to move its back-up data center operations to a new vendor. We reviewed the BCBSMS disaster recovery plan and discovered that it had not been updated to reflect the data center vendor change nor had the plan been tested to ensure that critical systems could be recovered at the new vendor's facility in the event of a disaster.

BCBSMS conducts business impact analyses (BIA) every three years, which are critical to determining what recovery strategies should be implemented. The next BIA update is due to take place in 2019. BCBSMS should utilize the results of the BIA to update its disaster recovery plan and then test the plan with the vendor to validate its effectiveness.

NIST SP 800-34, Revision 1, states, "As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan."

NIST SP 800-53, Revision 4, states that the organization should test its contingency plan for effectiveness and organizational readiness.

Failure to update and test contingency plans increases the risk that unexpected delays in restoring critical systems may occur in the event of a disaster.

Recommendation 9

We recommend that BCBSMS update its disaster recovery plan to incorporate the new vendor back-up data center.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS has revised disaster recovery documentation to bring them current and replaced all instances of [redacted]. This was completed June 30, 2019."

Recommendation 10

We recommend that BCBSMS test its disaster recovery plan at its new backup-data center.

BCBSMS's Response:

"BCBS agrees with this recommendation. BCBSMS will work to complete its disaster recovery test plan at its new backup location. The target implementation date is October 31, 2019."

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSMS's claims adjudication process. BCBSMS prices and adjudicates claims using an internally developed claims processing application called National Adjudication System and the Blue Cross Blue Shield Association's nationwide Federal Employee Program (FEP) Direct system. We reviewed the following processes related to claims adjudication: claims processing, application configuration management, and provider debarment.

1. Claims Processing System

We evaluated the business process controls associated with BCBSMS's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that BCBSMS 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 BCBSMS has not implemented adequate controls over its claims processing system.

2. Application Configuration Management

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

BCBSMS has implemented policies and procedures related to application configuration management, and has adopted a system development life cycle (SDLC) methodology that IT personnel follow during routine software modifications. However, the process for considering [redacted] within the SDLC process could be improved.

We asked BCBSMS personnel if [redacted] during the SDLC process; we were told [redacted]. BCBSMS stated that based on the results [redacted] We asked for evidence of historical changes where the [redacted] In response, we received [redacted]. However, [redacted]. We then reviewed BCBSMS's overarching Security Program Procedures document as well as a Change Control Process document to determine if either document required a [redacted]

NIST SP 800-64, Revision 2, states that [redacted]

NIST SP 800-128 states that [redacted]

NIST SP 800-53, Revision 4, provides guidance for which employees should [redacted]

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

[redacted]

Recommendation 11

We recommend that BCBSMS update its [redacted] be conducted by a qualified individual.

BCBSMS's Response:

"BCBSMS agrees with this recommendation. BCBSMS will work to [redacted] The target implementation date is October 31, 2019."

3. Debarment

BCBSMS has documented procedures for reviewing provider files for debarments and suspensions. BCBSMS's FEP department downloads the OPM OIG debarment list, formats it into a spreadsheet, and manually uploads the relevant information into FEP Direct. When the debarment list is updated, BCBSMS sends notification to any member who has seen a provider on the list. If a debarred provider submits a claim, this claims will hit an edit, to be reviewed by a claims processor. The processing guides used by BCBSMS include guidance on the 15-day OIG mandated grace period.

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

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

August 26, 2019

[redacted] Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management (OPM)
1900 E Street, NW
Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT IT AUDIT REPORT
Blue Cross Blue Shield of Mississippi (BCBSMS or the "Plan")
Audit Report Number 1A-10-40-19-010
(Dated June 5, 2019)

The following sets forth BCBSMS's response as it relates to OPM's recommendations included in the draft audit report referenced above.

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

1. Segregation of Duties

Recommendation 1

We recommend that BCBSMS develop policies and procedures to ensure that access to information systems is granted with proper segregation of duties.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to develop segregation of duties policies and procedures to leverage during access provisioning. The target implementation date is November 30, 2019.

C. NETWORK SECURITY

1. Documented Firewall Management Policy

Recommendation 2

We recommend that BCBSMS develop and maintain a detailed firewall management policy to provide guidance for [redacted] firewalls as well as approving and documenting changes.

Plan Response

BCBSMS agrees with this recommendation. [redacted]. This was completed July 31, 2019.

2. Firewall Configuration Review

Recommendation 3

We recommend that BCBSMS perform routine audits of its current firewall configurations against an approved firewall policy. Note – this recommendation cannot be implemented until the controls from Recommendation 2 are in place.

Plan Response

BCBSMS agrees with this recommendation. [redacted] This was completed July 31, 2019.

3. Network Segmentation

Recommendation 4

We recommend that BCBSMS [redacted]

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will continue to work on completing the [redacted]. The target implementation date is December 31, 2020.

4. Vulnerability Scanning

Recommendation 5

We recommend that BCBSMS ensure the scans are conducted with sufficient access to perform a thorough scan.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to ensure that adequate access to all systems, where applicable, is in place to perform thorough vulnerability scans. If full credentialed scans cannot be performed, a risk assessment will be conducted. The target implementation date is October 31, 2019.

5. OIG Vulnerability Scanning

Recommendation 6

We recommend that BCBSMS remediate the specific [redacted] discovered during this audit as outlined in the vulnerability scan audit inquiry.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to have all identified [redacted] remediated. The target implementation date is September 30, 2019.

D. CONFIGURATION MANAGEMENT

1. Security Configuration Standards

Recommendation 7

We recommend that BCBSMS [redacted]

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to [redacted] The target implementation date is October 31, 2019.

2. Security Configuration Auditing

Recommendation 8

We recommend that BCBSMS implement a process to [redacted]

Note – this recommendation cannot be implemented until the controls from Recommendation 7 are in place.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to [redacted]. The target implementation date is November 30, 2019.

E. CONTINGENCY PLANNING

1. Disaster Recovery Plan and Testing

Recommendation 9

We recommend that BCBSMS update its disaster recovery plan to incorporate the new vendor back-up data center.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS has revised disaster recovery documentation to bring them current and replaced all instances of [redacted]. This was completed June 30, 2019.

Recommendation 10

We recommend that BCBSMS test its disaster recovery plan at its new backup-data center.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to complete its disaster recovery test plan at its new backup location. The target implementation date is October 31, 2019.

F. Claims Adjudication

1. Application Change Control

Recommendation 11

We recommend that BCBSMS update its [redacted] be conducted by a qualified individual.

Plan Response

BCBSMS agrees with this recommendation. BCBSMS will work to have [redacted] The target implementation date is October 31, 2019.

BCBSMS appreciates the opportunity to respond to each of the recommendations in the draft report. Moreover, BCBSMS requests that its 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], 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