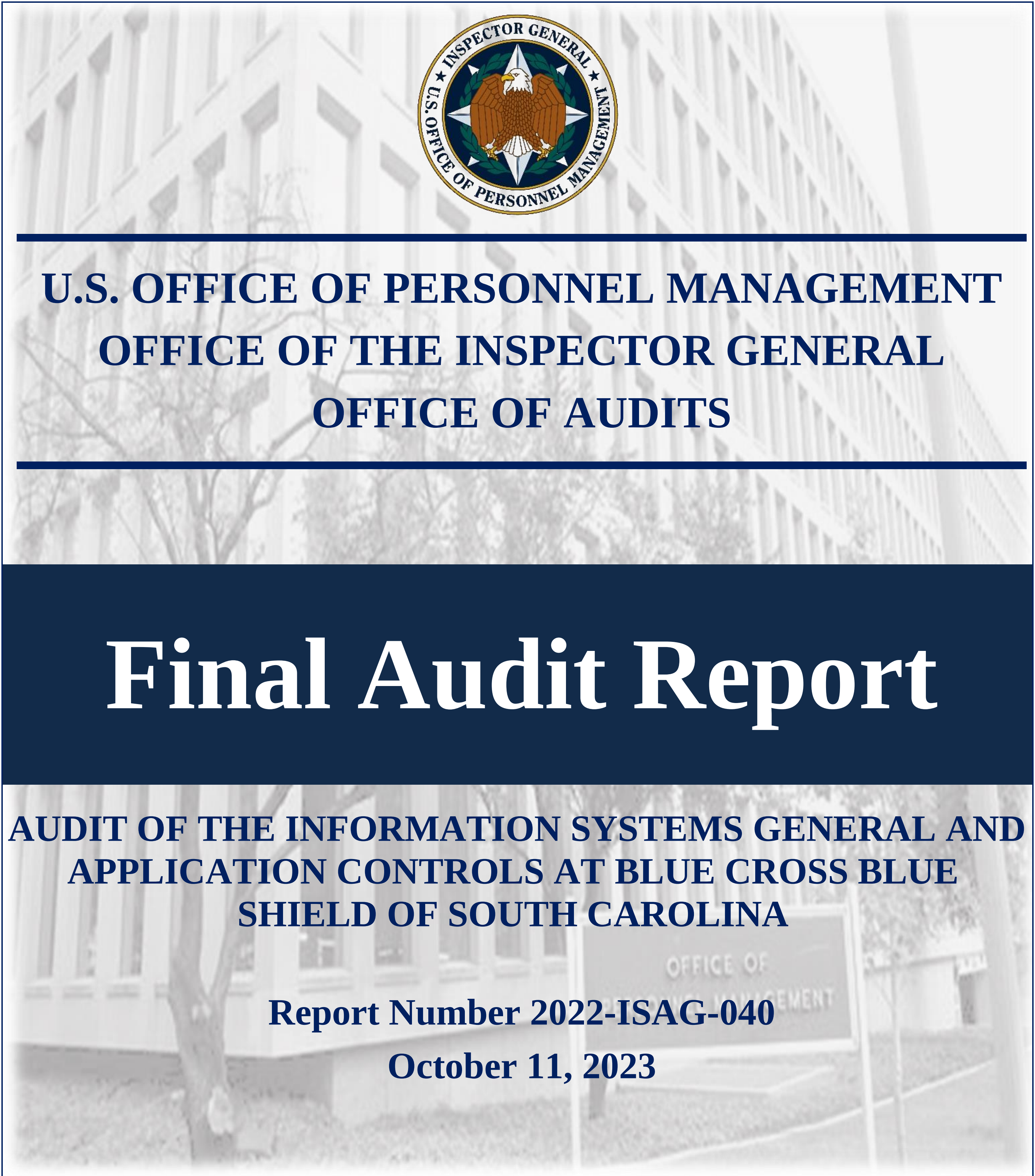

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

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

Report Number 2022-ISAG-040

October 11, 2023

– CAUTION –

This report has been distributed to Federal officials who are responsible for the administration of the subject program. This non-public version may contain confidential and/or proprietary information, and should not be further released unless authorized by the OIG.

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Blue Cross Blue Shield of South Carolina.

Report No. 2022-ISAG-040 **October 11, 2023**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of South Carolina (BCBSSC) is contracted by the U.S. Office of Personnel Management to provide health insurance benefits for Federal employees, annuitants, and their dependents as part of the Federal Employees Health Benefits Program (FEHBP).

The objective of this audit was to determine if BCBSSC has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

What Did We Audit?

The scope of this audit included all BCBSSC information systems operating in the general control environment where FEHBP data is processed and stored as of March 2023.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of BCBSSC's information technology security controls determined that:

- BCBSSC has an adequate enterprise management program in place.
- BCBSSC has sufficient controls for multi-factor authentication for privileged logical access.
- BCBSSC has implemented appropriate policies for both granting and removing of physical access.
- The BCBSSC data center has a long-term emergency generator and uninterruptable power supplies that provide power failover for all systems.
- BCBSSC conducts credentialed vulnerability and configuration compliance scans; [redacted].
- BCBSSC's enterprise security event monitoring and incident response programs are adequate.
- [redacted]
- [redacted]
- BCBSSC has adequate controls over its contingency planning program.
- BCBSSC has adequate system development lifecycle policies and procedures.

ABBREVIATIONS

BCBSSC	**Blue Cross and Blue Shield of South Carolina**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information Systems Controls Audit Manual**
GAGAS	**Generally Accepted Government Auditing Standards**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
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 Blue Cross and Blue Shield of South Carolina's (BCBSSC) general and application controls for its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data related to the following health insurance plan codes are processed and stored, as of March 2023:

- Blue Cross and Blue Shield Service Benefit Plan Standard Option – 10;
- Blue Cross and Blue Shield Service Benefit Plan Basic Option – 11; and
- Blue Cross and Blue Shield Service Benefit Plan FEP Blue Focus – 13.

The FEHBP was established by the Federal Employees Health Benefits Act (Public Law 86-382), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for Federal employees, annuitants, and their dependents. Health insurance coverage is made available through contracts with various health insurance carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

The provisions of the Federal Employees Health Benefits Act are implemented by the U.S. Office of Personnel Management (OPM) through regulations that are codified in Title 5, Chapter 1, Part 890 of the Code of Federal Regulations (CFR).

FEHBP contracts include provisions stating that an authorized representative of the Contracting Officer may use National Institute of Standards and Technology Special Publication (NIST SP) 800-53 (or its current equivalent) requirements as a benchmark for conducting audits of a health insurance carrier's information systems and may recommend that the carrier adopt a best practice drawn from NIST SP 800-53 (or its current equivalent) for information systems that directly process FEHBP data and all other information systems in the same general IT environment.

This audit was conducted pursuant to BCBSSC's FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 CFR Chapter 1, Part 890. The audit was performed by OPM's Office of the Inspector General (OIG), as established and authorized by the Inspector General Act of 1978, as amended (5 U.S.C. §§ 401-424).

This was our second audit of general and application controls at BCBSSC (Report No: 1A-10-24-11-014). All recommendations from the previous audit are closed. All BCBSSC 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 were greatly appreciated.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this audit was to determine if BCBSSC has implemented adequate general and application controls to protect the confidentiality, integrity, and availability of FEHBP data processed and stored by its information systems.

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States. GAGAS requires that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of this audit included all BCBSSC information systems operating in the general IT control environment where FEHBP data is processed and stored as of March 2023.

Due to resource limitations, we were not able to assess the entire BCBSSC information systems control environment. Therefore, the scope of our work was limited to high-risk areas identified during the planning phase of our audit. Accordingly, we performed a risk assessment of BCBSSC's information systems environment and applications during the planning phase of the audit to develop an understanding of BCBSSC's controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the controls were properly designed, placed in operation, and effective.

Our audit program was based on procedures and controls contained in the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) and NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

NIST SP 800-53 controls were selected for testing based on risk, applicability, and overall impact to the organization's IT security posture. These controls have been organized into the following audit sections:

- Enterprise Security;
- Logical Access;
- Physical Access;
- Data Center;
- Network Security;

- Security Event Monitoring and Incident Response;
- Configuration Management;
- Contingency Planning; and
- System Development Lifecycle.

For each of our audit sections, FISCAM identifies critical elements that represent tasks essential for establishing adequate controls. For each critical element, there is a discussion of the associated objectives, risks, and critical activities, as well as related control techniques and audit concerns.

NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, includes a comprehensive set of procedures for assessing the effectiveness of security and privacy controls defined in NIST SP 800-53. We used these potential assessment methods and artifacts, where appropriate, to evaluate BCBSSC's controls. This included interviews, observations, control tests, and inspection of computer-generated data and various documents, including IT and other related organizational policies and procedures.

When our objective involved the assessment of computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable. However, due to time constraints, we did not verify the reliability of data used to complete some of our audit steps when we determined that the evidence was adequate to achieve our audit objectives.

Control tests were performed to determine the extent to which established controls and procedures are functioning as intended. Where appropriate, control tests utilized judgmental sampling methods. Results of judgmentally selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included interviews of staff, documentation reviews, and testing of the general and application controls in place over BCBSSC's information systems. The business processes reviewed are primarily located in Columbia, South Carolina.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at BCBSSC as of March 2023.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether BCBSSC's information system general and application controls were consistent with applicable standards. Various laws, regulations, and industry standards were used as a guide to evaluate BCBSSC's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;
- NIST SP 800-53, Revision 5; and
- BCBSSC's policies and procedures.

While generally compliant with respect to the items tested, BCBSSC was not in compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. ENTERPRISE SECURITY

Enterprise security controls include the policies, procedures, and techniques that serve as the foundation of BCBSSC's overall IT security program. We evaluated BCBSSC's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSSC has adequate controls over Enterprise Security.

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

- Formalized information security and monitoring policies;
- Documented risk management methodology and remediation plans to address weaknesses identified in risk assessments; and
- Human resources policies and procedures related to specialized training and IT Security awareness.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate controls related to security management.

B. LOGICAL ACCESS

Logical access controls include the policies, procedures, and techniques used to detect and prevent unauthorized logical access to information systems or modification, loss, and disclosure of sensitive data. We evaluated the logical access controls protecting sensitive data on BCBSSC's network environment and applications supporting the FEHBP claims processing business function.

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

- Multi-factor authentication for privileged access;
- Routine reviews of access to critical systems; and
- Logical access is granted using the principle of least privilege.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate logical access controls.

C. PHYSICAL ACCESS

Physical access controls include the policies, procedures, and techniques used to prevent or detect unauthorized physical access to facilities which contain information systems and sensitive data. We evaluated the controls protecting physical access to BCBSSC's facilities and data centers.

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

- Documented policies and procedures for granting, removing, and adjusting physical access;
- Monitoring and response capabilities for physical security incidents; and
- Routine audits and physical access reviews to ensure that employee access is appropriate.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate physical access controls.

D. DATA CENTER

Data center controls include the policies, procedures, and techniques used to protect information systems from environmental damage and provide network resiliency. We evaluated the data center controls at BCBSSC's primary and back-up data centers.

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

- A long-term emergency generator and uninterruptable power supplies provide power failover for systems;
- Environmental controls to detect water leakage on the data center floor; and
- Scheduled preventative maintenance for fire suppression and detection systems.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate data center controls.

E. NETWORK SECURITY

Network security controls include the policies and procedures used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated BCBSSC'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.

BCBSSC [redacted]

We observed the following controls in place:

- Perimeter controls to secure connections to external networks.
- Network access controls to prevent unauthorized devices on the internal network; and
- Technical controls to secure endpoint devices.

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

1. Vulnerability Management

As a part of this audit, BCBSSC conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network on our behalf. [redacted]

The BCBSSC Operations Vulnerability Management policy states that vulnerability scans are to be performed on all systems at least weekly. [redacted]

[redacted]

NIST SP 800-53, Revision 5, control RA-5 Vulnerability Monitoring and Scanning, states that the organization should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

[redacted]

Recommendation 1

[redacted]

BCBSSC's Response:

[redacted]

OPM OIG Comment:

As part of the audit resolution process, BCBSSC should provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement also applies to all subsequent recommendations in this audit report that BCBSSC agrees to implement.

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting.

BCBSSC has an adequate event monitoring program.

We observed the following controls in place:

- Controls to monitor security events throughout the network;
- Policies and procedures for analyzing security events; and

- A documented incident response program.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate security event monitoring and incident response controls.

G. CONFIGURATION MANAGEMENT

Configuration management controls include the policies, procedures, and techniques used to develop, implement, and maintain secure, risk-based system configurations and ensure that systems are configured according to these standards. We evaluated BCBSSC's configuration management of its end-user devices, servers, databases.

[redacted]

We observed the following controls in place:

- Documented security configuration standards;
- Adequate change management separation of duty controls; and
- An adequate patch management process.

The following sections document opportunities for improvement related to BCBSSC's configuration management controls.

1. Patch Management

[redacted]

NIST SP 800-53, Revision 5, control RA-5 Vulnerability Monitoring and Scanning, states that the organization should scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities.

[redacted]

Recommendation 2

We recommend that BCBSSC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

BCBSSC's Response:

"BCBSSC agrees with the recommendation and, except in cases of business exceptions, will remediate the specific vulnerabilities identified."

2. Unsupported Software

[redacted]

NIST SP 800-53 Revision 5, control SA-22 Unsupported System Components, states that the organization should "Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer" or obtain extended support.

[redacted]

Recommendation 3

[redacted]

BCBSSC's Response:

"BCBSSC disagrees with this recommendation. The following documentation, taken together, captures our policies and procedures related to how unsupported software is replaced or supported beyond end-of-life:

- ***… BCBSSC's Cyber Security Framework policy that outlines system and services acquisition, including the requirement that unsupported system components are replaced by the business unit at end-of-life or provide justification and documentation for continued usage (p.6).***

- ***… the Application Systems Management section of the Information Systems Standards Manual specifically identifies software at end-of-life as being an example of "Nonstandard Hardware/Software Use." Furthermore, this documentation directs that nonstandard use must be approved by the Enterprise Architect Office following the procedure outlined within. This attachment was provided as part of the initial documentation request (7.4 ISSM Application Systems Management Volume).***

- ***… ITBSA Data General Desk Procedures and Instruction – BCBSSC's documented procedures for the Monitoring Observability Pipeline team. Included in this document, on page 4, is the directive for system expert or tool owners to semi-annually confirm that their software is still supported."***

OIG Comments:

In response to the draft audit report, we received evidence that the Cyber Security Framework Policy, Information Systems Standards Manual, and IT-Business Strategic Alignment Data General Desk Procedures and Instruction adequately define how unsupported software should be identified and managed; therefore, no further action is required.

Recommendation 4

[redacted]

BCBSSC's Response:

[redacted]

H. CONTINGENCY PLANNING

BCBSSC has adequate controls over contingency planning.

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

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

- Contingency plans including disaster recovery and business continuity plans;

- Contingency plan testing and follow-up; and
- Emergency response training.

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

I. SYSTEM DEVELOPMENT LIFECYCLE

System development lifecycle controls include the policies, procedures, and techniques related to the secure and controlled internal development of software supporting claims adjudication and sensitive web applications. We evaluated BCBSSC’s software development and change control policies and procedures and controls related to secure software development.

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

- An adequate application change review and approval process;
- Documented software development procedures; and
- Source code security and quality analyses for internally developed software.

Nothing came to our attention to indicate that BCBSSC has not implemented adequate system development lifecycle controls.

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 7, 2023

Louis Clement, 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 South Carolina (BCBSSC)
Audit Report Number 2023-ISAG-0040
(Dated June 6, 2023)

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

A. ENTERPRISE SECURITY

No recommendations noted.

B. LOGICAL ACCESS

No recommendations noted.

C. PHSYICAL ACCESS

No recommendations noted.

D. DATA CENTER

No recommendations noted.

E. NETWORK SECURITY

Vulnerability Management

Recommendation 1

[redacted]

Plan Response

[redacted]

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

No recommendation noted.

G. CONFIGURATION MANAGEMENT

Patch Management

Recommendation 2

We recommend that BCBSSC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.

Plan Response

BCBSSC agrees with the recommendation and, except in cases of business exceptions, will remediate the specific vulnerabilities identified.

Unsupported Software

Recommendation 3

[redacted]

Plan Response

BCBSSC disagrees with this recommendation. The following documentation, taken together, captures our policies and procedures related to how unsupported software is replaced or supported beyond end-of-life:

- **Attachment 1 – CSF 66016** – BCBSSC's Cyber Security Framework policy that outlines system and services acquisition, including the requirement that unsupported system components are replaced by the business unit at end-of-life or provide justification and documentation for continued usage (p.6).

- **Attachment 2 – ISSM 1.2.3** - the Application Systems Management section of the Information Systems Standards Manual specifically identifies software at end-of-life as being an example of “Nonstandard Hardware/Software Use.” Furthermore, this documentation directs that nonstandard use must be approved by the Enterprise Architect Office following the procedure outlined within. This attachment was provided as part of the initial documentation request (7.4 ISSM Application Systems Management Volume).
- **Attachment 3 – ITBSA Data General Desk Procedures and Instruction** – BCBSSC’s documented procedures for the Monitoring Observability Pipeline team. Included in this document, on page 4, is the directive for system expert or tool owners to semi-annually confirm that their software is still supported.

Recommendation 4

[redacted]

Plan Response

[redacted]

H. CONTINGENCY PLANNING

No recommendations noted.

I. SYSTEM DEVELOPMENT LIFECYCLE (SDLC)

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]

Sincerely,

Kim King
Managing Director, FEP Program Assurance

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: https://oig.opm.gov/contact/hotline

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100