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 BlueCross BlueShield of Tennessee

Report Number 2025-ISAG-009
October 14, 2025

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at
BlueCross BlueShield of Tennessee

Report No. 2025-ISAG-009 **October 14, 2025**

Why Did We Conduct the Audit?

BlueCross BlueShield of Tennessee (BCBST) is contracted by the U.S. Office of Personnel Management to provide health insurance benefits for federal employees, annuitants, and their eligible dependents as part of the Federal Employees Health Benefits Program (FEHBP).

The objective of this audit was to determine if BCBST 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 BCBST information systems operating in the general control environment where FEHBP data is processed and stored as of June 2025.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of BCBST's information systems general and application controls determined that:

- BCBST [redacted]
- BCBS [redacted]
- BCBST [redacted]
- BCBST did not provide sufficient evidence for how it determines which roles require separation during its logical access provisioning and review processes. However, BCBST is deploying a new Identity and Access Management tool that will provide granular separation of duties.
- BCBST has implemented adequate physical access controls.
- BCBST does not have a formalized policy to secure, inventory, or regularly change keys to the data center.
- BCBS [redacted]
- Our testing identified that [redacted]
- BCBST [redacted]
- BCBST has developed adequate documented disaster recovery and business continuity plans.
- BCBST performs adequate developer testing and evaluation.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
BCBST	**Blue Cross Blue Shield of Tennessee**
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**
IAM	**Identity and Access Management**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
SP	**Special Publication**
SCRM	**Supply chain risk management**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of BlueCross BlueShield of Tennessee's (BCBST) general and application controls over its information systems operating in the general information technology (IT) control environment where Federal Employees Health Benefits Program (FEHBP) data is processed and stored as of June 2025.

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 eligible 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 Office may use National Institute of Standards and Technology (NIST) Special Publication (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) to information systems that directly process FEHBP data and all other information systems in the same general IT environment.

The audit was conducted pursuant to BCBST 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.

This was the second audit of the information systems general and application controls at BCBST. The previous audit of general and application controls at BCBST was conducted in 2013 and Final Audit Report No. 1A-10-15-13-002 was issued on August 6, 2013. All recommendations from the previous audit have been closed.

All BCBST 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 BCBST has implemented adequate general and application controls over its information systems to protect the confidentiality, integrity, and availability of FEHBP data.

SCOPE AND METHODOLOGY

This audit was a performance audit 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 BCBST information systems operating in the general IT control environment where FEHBP data is processed and stored as of June 2025.

Due to resource limitations, we were not able to assess the BCBST's entire 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 BCBST's information systems environment and applications during the planning phase of the audit to develop an understanding of BCBST's internal controls. Using this risk assessment, additional audit steps were developed, as appropriate, to verify that the internal controls were properly designed, placed in operation, and effective.

The audit program was based on procedures contained in the 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, Revision 5, 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, Revision 5. We used these potential assessment methods and artifacts, where appropriate, to evaluate BCBST's internal controls. This includes 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.

All audit work was completed remotely. The remote work performed included staff interviews, documentation reviews, and testing of the general and application controls in place over BCBST's information systems. The business processes reviewed are primarily located in Chattanooga, Tennessee.

The findings, recommendations, and conclusions outlined in this report are based on the status of information systems general and application controls in place at BCBST as of June 2025.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether BCBST'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 BCBST's control structure.

These criteria included, but were not limited to, the following publications:

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

While generally compliant with respect to the items tested, BCBST 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 BCBST's overall IT security program. We evaluated BCBST's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

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

- Documented enterprise security policies and procedures;
- Routine information security risk assessments; and
- Routine security awareness training.

However, we identified the following opportunities for improvement related to BCBST's enterprise security controls.

1. Supply Chain Risk Management Plan

Supply chain risk management (SCRM) plans include risk tolerance for the organization, acceptable mitigation strategies, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, and SCRM roles and responsibilities. Further, a SCRM plan addresses requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems.

NIST SP 800-53, Revision 5, control SR-2, states that an organization should "Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services … ."

Recommendation 1

We recommend that BCBST [redacted]

BCBST Response:

"BCBST acknowledges the Supply Risk Management (SRM) recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

OIG Comment:

As a part of the audit resolution process, please provide OPM's Audit Resolution and Compliance office with evidence that BCBST has fully implemented this recommendation. This statement also applies to the subsequent recommendations in this audit report that BCBST agrees to implement.

Recommendation 2

We recommend that BCBST [redacted].

Note – this recommendation cannot be implemented until the controls from Recommendation 1 are in place.

BCBST Response:

"BCBST acknowledges the [Supply Risk Management (SRM)] recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

2. Supply Chain Controls and Processes

Supply chain elements include organizations, entities, or tools used for the design, acquisition, delivery, integration, operation, and disposal of systems and system components. Supply chain processes include hardware, software, the firmware development process, configuration management tools, and shipping and handling. Supply chain elements and processes may be provided by organizations, system

integrators, or external providers. BCBST [redacted]

NIST SP 800-53, Revision 5, control SR-3, states that the organization "Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements … ."

[redacted]

Recommendation 3

We recommend that BCBST [redacted]

BCBST Response:

"BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

Recommendation 4

We recommend that BCBST [redacted].

Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

BCBST Response:

"BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

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 BCBST's network environment and applications supporting the FEHBP claims processing business function.

BCBST could improve its service account management and separation of duties controls.

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

- Multifactor authentication for remote users;
- Enforcement of a limit on consecutive invalid logon attempts; and
- Prevention of non-privileged users from executing privileged functions.

However, we identified the following opportunities for improvement related to BCBST's logical access controls.

1. Account Management

BCBST has developed standards that define its requirements for logical access account management. The standards include security controls applicable to service accounts. However, [redacted].

NIST SP 800-53, Revision 5, control AC-2, states that organizations should "Review accounts for compliance with account management requirements … ."

Failure to review service accounts increases the risk that service accounts are not in compliance with account management requirements.

Recommendation 5

We recommend that BCBST develop a process and frequency to review service accounts.

BCBST Response:

"BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

Recommendation 6

We recommend that BCBST review its service accounts for compliance with account management requirements.

Note – this recommendation cannot be implemented until the controls from Recommendation 5 are in place.

BCBST Response:

"BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

2. Separation of Duties

Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. We were provided with evidence [redacted] Yet, BCBST was unable to provide sufficient evidence for how it determines which roles require separation during its logical access provisioning and review processes. BCBST informed us that it is deploying a new IAM tool that will provide granular separation of duties [redacted]

NIST SP 800-53, Revision 5, control AC-5, states that organizations "Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and Define system access authorizations to support separation of duties." Further, AC-6 states that organizations "Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks." Additionally, the BCBST [redacted]

[redacted]

Failure to identify and document the organization-defined duties of individuals that require separation increases the potential for abuse of authorized privileges.

Recommendation 7

We recommend that BCBST [redacted]

BCBST Response:

"BCBST acknowledges the separation of duties recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

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 BCBST facilities.

BCBST performs routine audits and reviews to ensure appropriate employee access.

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

- Adequate physical security controls employed at BCBST facilities;
- Documented policies and procedures for managing physical access of employees and contractors; and
- Routine audits and reviews of employee and contractor access to BCBST facilities.

Nothing came to our attention to indicate that BCBST 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 unauthorized physical access, environmental damage, and provide network resiliency. We evaluated the data center controls at BCBST's primary and back-up data centers.

BCBST does not have a formalized policy to secure, inventory or regularly change keys to the data center.

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

- Physical access is monitored at the facility where the systems reside;
- Environmental controls maintain temperature and humidity; and
- Fire detection and suppression systems are in place.

However, we noted the following opportunity for improvement related to BCBST's data center controls.

1. Physical Access – Data Center

[redacted] owever, BCBST does not have a formalized policy to secure, inventory or regularly change keys to the data center.

NIST SP 800-53, Revision 5, control PE-1, states that the organization should develop and implement a "physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and … 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls … ."

Failure to document policies and procedures for securing, inventorying, and regularly changing data center keys increases the risk that unauthorized individuals may gain access to the data center, leading to possible data breaches and/or system compromise.

Recommendation 8

We recommend that BCBST create a formal key management policy that defines procedures for securing, inventorying, and regularly changing data center keys.

BCBST's Response:

"BCBST acknowledges the data center access finding and took immediate steps to begin the remediation during fieldwork. Remediation was completed by June 13, 2025, when the new Data Center Access Door Lock & Key Replacement Policy was published in the company policy and procedure repository (Attachment 1)."

OIG Response

In response to the draft report, we received evidence of an implemented Data Center Access Door Lock & Key Replacement Policy. The intent of the recommendation has been met. No further action is required.

E. NETWORK SECURITY

Network security controls include the policies, procedures, and techniques used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources. We evaluated BCBST controls related to network design, data protection, and systems monitoring.

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

- Firewalls inspecting and filtering BCBST's network traffic;
- Technical controls to monitor and manage emails and web connections; and
- Adequate security controls to protect data stored online.

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

1. Network Access Control

BCBS [redacted] 

[redacted].

NIST SP 800-53, Revision 5, control AC-17, states that organizations should "Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed … ."

Additionally, NIST SP 800-41, Revision 1, states that a common firewall requirement is performing "client checks for incoming connections from remote users and allow or

disallow access based on those checks. This checking, commonly called network access control or network access protection, allows access based on the user's credentials and the results of performing 'health checks' on the user's computer."

[redacted]

Recommendation 9

We recommend that BCBST [redacted]

BCBST Response:

"BCBST acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it."

2. Vulnerability Management

As a part of this audit, BCBST conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network on our behalf. We chose a judgmental sample of [redacted]. The sample included a variety of system functionality and operating systems across production, test, and development environments. The sample was judgmentally selected from systems that store and/or process FEHBP data. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

The specific vulnerabilities that we identified were provided to BCBST in the form of an audit inquiry. [redacted].

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

NIST SP 800-53, Revision 5, control SA-22, 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.

NIST SP 800-53, Revision 5, control SI-2, states that the organization should "Install security-relevant software and firmware updates within [… [the] organization-defined time period] of the release of the updates … ."

[redacted]

Recommendation 10

We recommend that BCBST [redacted]

BCBST Response:

"BCBST acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close the remaining items open in Kenna."

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Security event monitoring controls include the policies, procedures, and techniques used for 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 controls include the policies, procedures, and techniques used to establish and implement an incident response plan which defines roles and responsibilities, response procedures, training, and reporting. We evaluated BCBST's controls related to event log collection and security incident detection, response, and reporting.

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

- A documented incident response program;
- A series of tools monitoring the availability, performance, and security of BCBST's network; and
- Adequate policies and procedures for triaging and investigating security alerts.

However, we identified the following opportunity for improvement related to BCBST's security event monitoring and incident response controls.

1. Encrypted Traffic Inspection

BCBST [redacted]

NIST SP 800-53, Revision 5, control SI-4, states organizations should make provisions so that encrypted communication traffic is visible to the organization's system monitoring tools and mechanisms.

NIST SP 800-53, Revision 5, control SI-4, states organizations should "[p]rovide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices."

[redacted]

Recommendation 11

We recommend BCBST [redacted]

BCBST Response:

"BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it."

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 BCBST's configuration management of its end-user devices, servers, and databases.

BCBST has implemented adequate controls related to configuration management.

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

- Established configuration change control policies and procedures;
- Routine compliance monitoring; and
- Utilization of tools to detect and implement patches/updates.

Nothing came to our attention to indicate that BCBST has not implemented adequate configuration management controls.

H. CONTINGENCY PLANNING

BCBST has implemented adequate contingency planning controls.

Contingency planning controls include the policies, procedures, and techniques that ensure continuity and recovery of critical business operations and the protection of data in the event of a service impacting event. We evaluated BCBST's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when service impacting events occur.

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

- Documented disaster recovery and business continuity plans;
- Routine contingency plan testing; and
- Policies and procedures to facilitate system backups.

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

I. SYSTEM DEVELOPMENT LIFECYCLE

BCBST has implemented adequate system development lifecycle controls.

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 BCBST'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:

- Documented software change management policies;
- Documented software development procedures; and
- Performance of adequate developer testing and evaluation.

Nothing came to our attention to indicate that BCBST 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
750 9th Street NW
Washington, D.C. 20001
202.942.1000
Fax 202.942.1125

August 20, 2025

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 Tennessee (BCBST)
Audit Report Number 2025-ISAG-009
(Dated June 27, 2025)

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

A. ENTERPRISE SECURITY

Supply Chain Risk Management Plan

Recommendation 1

We recommend that BCBST [redacted]

Plan Response

BCBST acknowledges the Supply Risk Management (SRM) recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

Recommendation 2

We recommend that BCBST [redacted]

Note – this recommendation cannot be implemented until the controls from Recommendation 1 are in place.

Plan Response

BCBST acknowledges the supply chain risk recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

Supply Chain Controls and Processes

Recommendation 3

We recommend that BCBST [redacted]

Plan Response

BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

Recommendation 4

We recommend that BCBST [redacted]

Note – this recommendation cannot be implemented until the controls from Recommendation 3 are in place.

Plan Response

BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

B. LOGICAL ACCESS

Account Management

Recommendation 5

We recommend that BCBST develop a process and frequency to review service accounts.

Plan Response

BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

Recommendation 6

We recommend that BCBST review its service accounts for compliance with account management requirements.

Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place

Plan Response

BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

Separation of Duties

Recommendation 7

We recommend that [redacted].

Plan Response

BCBST acknowledges the separation of duties recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

C. PHSYICAL ACCESS

No recommendations noted.

D. DATA CENTER

Physical Access – Data Center

Recommendation 8

We recommend that [redacted]

Plan Response

BCBST acknowledges the data center access finding and took immediate steps to begin the remediation during fieldwork. Remediation was completed by June 13, 2025, when the new Data Center Access Door Lock & Key Replacement Policy was published in the company policy and procedure repository (**Attachment 1**).

E. NETWORK SECURITY

Network Access Control

Recommendation 9

We recommend that [redacted]

Plan Response

BCBST acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close it.

Vulnerability Management

Recommendation 10

We recommend that [redacted]

Plan Response

BCBST acknowledges this recommendation and will work with OPM Audit Compliance and Resolution to close [redacted]

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Encrypted Traffic Inspection

Recommendation 11

We recommend BCBST [redacted]

Plan Response

BCBST acknowledges the recommendation and self-identified this prior to the audit. BCBST has a project already active to remediate this finding and will work with OPM Audit Compliance and Resolution to close it.

G. CONFIGURATION MANAGEMENT

No recommendations noted.

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] at [redacted]

Sincerely,

[redacted]

Kim King
Managing Director, FEP Program Assurance

cc: Eric Keehan, 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: 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