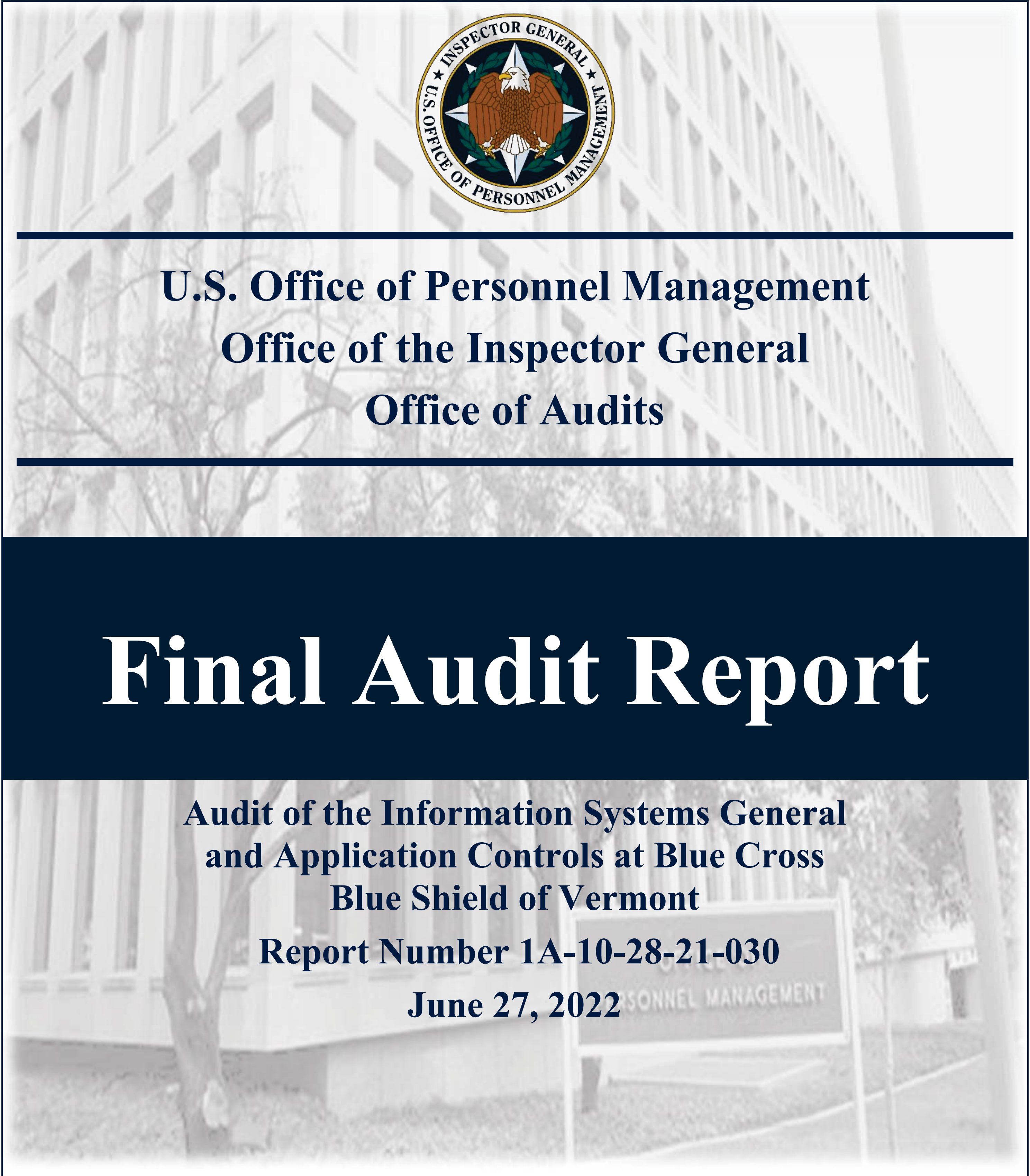

U.S. Office of Personnel Management
Office of the Inspector General
Office of Audits

Final Audit Report

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

Report Number 1A-10-28-21-030

June 27, 2022

Executive Summary

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

Report No. 1A-10-28-21-030 **June 27, 2022**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of Vermont (BCBSVT) 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 BCBSVT's information technology (IT) environment.

What Did We Audit?

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

- BCBSVT has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified during risk assessments. BCBSVT also performs risk assessments of its third-party vendors.
- BCBSVT has adequate physical and logical access controls in place to grant, adjust, and remove access to facilities and information systems.
- BCBSVT has perimeter controls in place to protect against external threats. However, [redacted]
- BCBSVT could improve internal segmentation between user and server networks. Additionally, there isn't a documented policy or procedure related to end-of-life software.
- BCBSVT could improve controls related to [redacted]
- BCBSVT has an established incident response program.
- BCBSVT has [redacted] BCBSVT also does not document [redacted].
- BCBSVT has contingency plans in place for claims-related operations.
- BCBSVT has documented and implemented an application change control process.

Abbreviations

BCBSVT	**Blue Cross Blue Shield of Vermont**
CFR	**Code of Federal Regulations**
CM	**Configuration Management**
FEHBP	**Federal Employees Health Benefits 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'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 general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Blue Cross Blue Shield of Vermont (BCBSVT).

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 initial audit of the information technology (IT) general security and application controls at BCBSVT. All BCBSVT 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. 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 BCBSVT's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Security event monitoring and incident response;
- Configuration management;
- Contingency planning; and
- Application controls specific to BCBSVT'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 BCBSVT's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of BCBSVT'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 BCBSVT to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Montpelier, Vermont.

Due to social distancing guidance related to COVID-19, all audit work was completed remotely. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general controls in place over BCBSVT's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at BCBSVT as of November 2021.

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

We used judgmental, random selection, or statistical sampling methods as appropriate throughout the audit. Results of judgmentally or randomly selected samples cannot be projected to the population since it is unlikely that the results are representative of the population as a whole.

In conducting this audit, we:

- Performed a risk assessment of BCBSVT'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);

- Gathered documentation and conducted interviews;

- Reviewed BCBSVT's business structure and environment; and

- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended.

Various laws, regulations, and industry standards were used as a guide in evaluating BCBSVT's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;

- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-41, Revision 1, Guidance on Firewalls and Firewall Policy.

Compliance with Laws and Regulations

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

BCBSVT has developed adequate IT security policies and procedures. BCBSVT has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSVT has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

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

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

- Documented policies and procedures for granting, removing, and adjusting physical access;
- Environmental and monitoring controls for the data center; and
- Documented policies and procedures for granting and removing logical access.

Nothing came to our attention to indicate that BCBSVT has not implemented adequate physical or logical access controls.

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

We observed the following controls in place:

- Preventive controls at the network perimeter;
- Adequate remote access controls; and
- Internal controls to filter web content.

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

1. [redacted] Network Segmentation

BCBSVT employs firewalls, intrusion prevention systems, virtual private networks, web application firewalls, and a demilitarized zone to secure connections between internal and external networks. [redacted]

[redacted]

[redacted]

Recommendation 1:

We recommend that BCBSVT complete its current project [redacted]

BCBSVT's Response:

"BCBSVT agrees with the recommendation. We are actively working on this project and anticipate its completion by [redacted]***, 2022."***

OIG Comments:

As part of the audit resolution process, we recommend that BCBSVT 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 BCBSVT agrees to implement.

2. Data Encryption at Rest

BCBSVT developed a data encryption standard requiring the use of strong encryption algorithms to protect the confidentiality of information when deemed necessary by risk analysis. However, BCBSVT does not enforce encryption at rest for systems that process Federal member data. BCBSVT is currently in the process of implementing a control to remediate this risk.

NIST SP 800-53, Revision 5, requires organizations to protect the confidentiality and/or integrity of information at rest using cryptographic mechanisms.

Failure to encrypt [redacted] increases the likelihood of data loss via unauthenticated malicious code.

Recommendation 2:

We recommend that BCBSVT complete its current project [redacted].

BCBSVT's Response:

"BCBSVT agrees with the recommendation. We are actively working on this project and anticipate its completion by [redacted]***, 2022."***

3. Vulnerabilities Identified by OIG Scans

BCBSVT conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. To conduct the vulnerability and compliance scan exercise, we chose a sample of [redacted] from a universe of [redacted]. The sample selection included a variety of system functionality and operating systems across production, test, development, and disaster recovery environments. The judgmental sample was drawn from systems that store, process, or forward federal member data, as well as other systems in the same general control environment that contain federal member 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 BCBSVT in the form of an audit inquiry but will not be detailed in this report. Our review of the scan results identified [redacted] BCBSVT is actively tracking and remediating [redacted] and has established remediation dates.

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

Furthermore, FISCAM states that "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective."

Failure to remediate vulnerabilities in a timely manner increases the risk that threat actors could exploit system weaknesses for malicious purposes.

Recommendation 3:

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

BCBSVT's Response:

"BCBSVT agrees with the recommendation. We have remediated all but two and provided evidence in Attachment 1. The remaining two will be remediated by [redacted], 2022."

OIG Comments:

In response to the draft audit report, BCBSVT provided evidence that it has remediated some of the technical weaknesses found during the scanning exercise. We continue to recommend that BCBSVT remediate the remaining technical weaknesses discovered during the audit.

4. System Lifecycle Management

BCBSVT does not have [redacted]. We reviewed many BCBSVT policies and procedures related to configuration management, however, [redacted] described how BCBSVT [redacted] system software components. Our review of the vulnerability scan results and BCBSVT's system inventory identified [redacted]

[redacted]

[redacted]

[redacted]

Recommendation 4:

We recommend that BCBSVT develop and implement a policy and procedures [redacted]

BCBSVT's Response:

"BCBSVT has agreed and implemented the recommendation. We have implemented this response by [redacted] ***(Attachment 2) and initiating the process*** [redacted] ***(Attachment 3)."***

OIG Comments:

In response to the draft audit report, BCBSVT provided evidence that it has updated guidance to ensure information systems are upgraded prior to the end of vendor support; no further action is required.

D. 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.

Our review of BCBSVT's security event monitoring and incident response programs identified 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 BCBSVT has not implemented adequate security event monitoring and incident response controls.

E. 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. BCBSVT employs a team of technical personnel who manage system software configuration for the organization. We evaluated BCBSVT's management of the configuration of its computer servers and databases.

We observed the following controls in place:

- Documented system hardening procedures;
- Documented security configuration standards; and
- Routine configuration auditing.

However, we noted the following opportunities for improvement related to BCBSVT's configuration management program.

1. Configuration Change Control Guidance

BCBSVT does not have a policy or procedures which adequately describe its current system configuration change control process. BCBSVT provided a document describing its old project management methodology which included guidance for configuration change control. However, there is no comparable document which describes the current process. BCBSVT is currently in the draft stage of creating a new project management methodology document.

NIST SP 800-53, Revision 5, states that the organization should develop and document configuration management policy and "Procedures to facilitate the implementation of the configuration management (CM) policy and the associated CM controls," which includes the requirements of CM-3 Configuration Change Control.

NIST SP 800-53, Revision 5, states that "Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications." NIST SP 800-53, Revision 5, also states, "Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes"

Failure to develop, document and disseminate configuration management policies and procedures increases the risk of unauthorized modifications or additions to the applications and to system components, leading to unauthorized access to data and applications.

Recommendation 5:

We recommend that BCBSVT develop configuration management policy and procedures to facilitate the implementation of all change control requirements.

BCBSVT's Response:

"BCBSVT has agreed and implemented the recommendation. Refer to Attachment 4 for the finalized Project Management Methodology Document."

OIG Comments:

In response to the draft audit report, BCBSVT provided evidence that it has developed a change control policy for project management; no further action is required.

2. Security Configuration Settings

BCBSVT has established security configuration standards for each operating system [redacted]

NIST SP 800-53, Revision 5, states that the organization should [redacted]

Failure to adequately document configuration settings could lead to inconsistently applied security configurations.

Recommendation 6:

We recommend that BCBSVT [redacted] to the published standards used for system configuration.

BCBSVT's Response:

"BCBSVT has agreed and implemented the recommendation. Refer to Attachment 5 for evidence that [redacted]***."***

OIG Comments:

In response to the draft audit report, BCBSVT provided evidence that it has approved system configuration exceptions identified during the scanning exercise; no further action is required.

F. Contingency Planning

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed BCBSVT's contingency planning documentation and processes to prevent or minimize interruptions to business operations if disruptive events were to occur. We identified the following controls in BCBSVT's contingency planning process:

- Contingency plans including disaster recovery and business continuity plans;
- Contingency plan testing and follow-up; and
- A documented data backup process.

Nothing came to our attention to indicate that BCBSVT has not implemented adequate controls over the contingency planning process.

G. Application Change Control

We evaluated BCBSVT's application development and change control process. BCBSVT utilizes third parties to develop and make changes to its claims processing applications. However, BCBSVT has implemented policies and procedures which govern its application change request and configuration management process.

We observed the following controls in place:

- Documented application change management policy;
- Application change review and approval process; and

- Application change documentation tracking.

Nothing came to our attention to indicate that adequate controls have not been implemented for the application change control 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

March 18, 2022

Martin Wiley, 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
BlueCross BlueShield of Vermont (BCBSVT)
Audit Report Number 1A-10-28-21-030
(Dated January 20, 2022)

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

A. Security Management

No recommendation noted.

B. Access Controls

No recommendation noted.

C. Network Security

Internal Network Segmentation

Recommendation 1:

We recommend that BCBSVT complete its current project [redacted]

Plan Response:

BCBSVT agrees with the recommendation. We are actively working on this project and anticipate its completion by [redacted], 2022.

Data Encryption at Rest

Recommendation 2:

We recommend that BCBSVT complete its current project for [redacted]

Plan Response

BCBSVT agrees with the recommendation. We are actively working on this project and anticipate its completion by [redacted], 2022.

Vulnerabilities Identified by OIG Scans

Recommendation 3:

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

Plan Response:

BCBSVT agrees with the recommendation. We have remediated all but two and provided evidence in **Attachment 1**. The remaining two will be remediated by [redacted], 2022.

System Lifecycle Management

Recommendation 4:

We recommend that BCBSVT develop and implement a policy and procedures [redacted]

Plan Response:

BCBSVT has agreed and implemented the recommendation. We have implemented this response by [redacted] (**Attachment 2**) and initiating the process [redacted] (**Attachment 3**).

D. Security Event Monitoring and Incident Response

No recommendation noted.

E. Configuration Management

Configuration Change Control Guidance

Recommendation 5:

We recommend that BCBSVT develop configuration management policy and procedures to facilitate the implementation of all change control requirements.

Plan Response:

BCBSVT has agreed and implemented the recommendation. Refer to **Attachment 4** for the finalized Project Management Methodology Document.

Security Configuration Settings

Recommendation 6:

We recommend that BCBSVT [redacted] to the published standards used for system configuration.

Plan Response:

BCBSVT has agreed and implemented the recommendation. Refer to **Attachment 5** for evidence that [redacted]

F. Contingency Planning

No recommendation noted.

G. Application Change Control

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,

[redacted]

Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
[redacted]

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