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 EXCELLUS BLUECROSS BLUESHIELD

Report Number 2024-ISAG-020
June 30, 2025

EXECUTIVE SUMMARY

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

Report No. 2024-ISAG-020 **June 30, 2025**

Why Did We Conduct the Audit?

Excellus BlueCross BlueShield (Excellus) 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 Excellus 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 Excellus information systems operating in the general control environment where FEHBP data is processed and stored as of January 2025.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

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

- Excellus conducts routine information security risk assessments.
- Excellus has implemented adequate logical access controls.
- Excellus has implemented adequate physical access controls.
- Excellus has sufficient environmental controls to maintain desired temperature and humidity throughout its data center.
- The Office of the Inspector General's testing identified that some Excellus systems are [redacted]
- Excellus has implemented adequate security event monitoring and incident response controls.
- Excellus has a documented configuration management policy and security configuration standards.
- Excellus has sufficient policies and procedures to facilitate system backups.
- Excellus has implemented adequate application change review and approval process controls.

ABBREVIATIONS

CFR	**Code of Federal Regulations**
Excellus	**Excellus BlueCross BlueShield**
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	**National Institute of Standards and Technology**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
SP	**Special Publication**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of Excellus BlueCross BlueShield's (Excellus) 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 January 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 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. They 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 Excellus'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.

This was our initial audit of the information systems general and application controls at Excellus. All Excellus personnel that worked with our staff 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 Excellus 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 Excellus information systems operating in the general IT control environment where FEHBP data is processed and stored as of January 2025.

Due to resource limitations, we were not able to assess Excellus'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 Excellus's information systems environment and applications during the planning phase of the audit to develop an understanding of Excellus'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 Excellus'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 Excellus's information systems. The business processes reviewed are primarily located in Rochester, New York.

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

COMPLIANCE WITH LAWS AND REGULATIONS

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

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

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

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

III. AUDIT FINDINGS AND RECOMMENDATION

A. ENTERPRISE SECURITY

Excellus has implemented adequate enterprise security controls.

Enterprise security controls include the policies, procedures, and techniques that serve as the foundation of Excellus's overall IT security program. We evaluated Excellus'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 policies and procedures;
- Routine information security risk assessments; and
- Routine security awareness training.

Nothing came to our attention to indicate that Excellus has not implemented adequate enterprise security controls.

B. LOGICAL ACCESS

Excellus provisions logical access based on a least privilege methodology.

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

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

- Multifactor authentication for remote users;
- Logical access accounts are adequately disabled; and
- Least privilege methodology for granting access to systems and applications.

Nothing came to our attention to indicate that Excellus 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 Excellus's facilities and data centers.

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

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

- Physical access to facilities is controlled using a badge access system;
- Documented policies and procedures for granting, removing, and adjusting physical access; and
- Routine audits and reviews are performed to ensure that employee access is appropriate.

Nothing came to our attention to indicate that Excellus 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 Excellus's primary and back-up data centers.

Excellus has implemented adequate data center controls.

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

- Generators and uninterruptible power supplies to maintain electrical power;
- Environmental controls to maintain desired temperature and humidity; and
- Fire detection and suppression systems are in place.

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

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 Excellus's controls related to network design, data protection, and systems monitoring.

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

- Internal and external facing firewalls;
- Network access controls to prevent unauthorized devices from connecting to the internal network; and
- Policies and procedures for vulnerability management.

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

1. OIG Vulnerability Scan Results

Excellus conducted credentialed vulnerability scans on a sample of servers and workstations in its network on our behalf. [redacted] The sample included a variety of system functionality and operating systems across the production, test, and development environments. The judgmental sample was selected from systems that store and/or process FEHBP data, as well as other systems in the same general control environment that contain 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 Excellus in the form of an audit inquiry but will not be detailed in this report. Our review of the scan results identified various instances [redacted] In response to this finding, Excellus stated it was aware of the vulnerabilities and is actively working to remediate the issues.

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."

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 … ."

Failure to identify and remediate vulnerabilities in a timely fashion [redacted]

Recommendation 1

We recommend that Excellus remediate the technical weaknesses outlined in the audit inquiry.

Excellus's Response:

"Excellus has an ongoing program to address the technical weaknesses identified in the audit inquiry. Excellus has remediated, risk accepted or provided evidence [of] false positives for the identified technical weaknesses."

OIG Comment:

Although some of the items were addressed in the audit inquiry response, as a part of the audit resolution process, please provide OPM's Audit Resolution and Compliance office with evidence that Excellus has fully implemented this recommendation.

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Excellus has implemented adequate controls related to 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 Excellus'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:

- Controls to monitor security events throughout the network;

- Documented incident response plans and playbooks; and
- Routine incident response testing.

Nothing came to our attention to indicate that Excellus 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 Excellus's configuration management of its end-user devices, servers, and databases.

Excellus has implemented adequate controls related to configuration management.

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

- Established configuration management policy;
- Documented security configuration standards; and
- Routine security configuration compliance monitoring.

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

H. CONTINGENCY PLANNING

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 Excellus's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when service impacting events occur.

Excellus has implemented adequate contingency planning controls.

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 Excellus 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 Excellus's software development and change control policies and procedures and controls related to secure software development.

Excellus has implemented adequate system development lifecycle controls.

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

- Documented software change management policies;
- Documented software development procedures; and
- Application change review and approval process.

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

APPENDIX

BlueCross BlueShield Association
Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005

April 11, 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

Plan: Excellus BlueCross BlueShield (Excellus BCBS)

Audit Report Number: 2024-ISAG-020 (Dated February 20, 2025)

The following represents Excellus BCBS'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

OIG Vulnerability Scan Results

Recommendation 1

We recommend that Excellus remediate the technical weaknesses outlined in the audit inquiry.

Plan Response

Excellus has an ongoing program to address the technical weaknesses identified in the audit inquiry. Excellus has remediated, risk accepted or provided evidence false positives for the identified technical weaknesses. Refer to documentation provided in **Attachment 1 – R1 Vulnerability Scan Results**.

F. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

No recommendations noted.

G. CONFIGURATION MANAGEMENT

No recommendations noted.

H. CONTINGENCY PLANNING

No recommendations noted.

I. SYSTEM DEVELOPMENT LIFECYCLE (SDLC)

No recommendations 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 Hoan Mai at [redacted]

Sincerely,

[redacted]

Kim King
Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
Hoan Mai, FEP
Amanda Tucker, 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

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