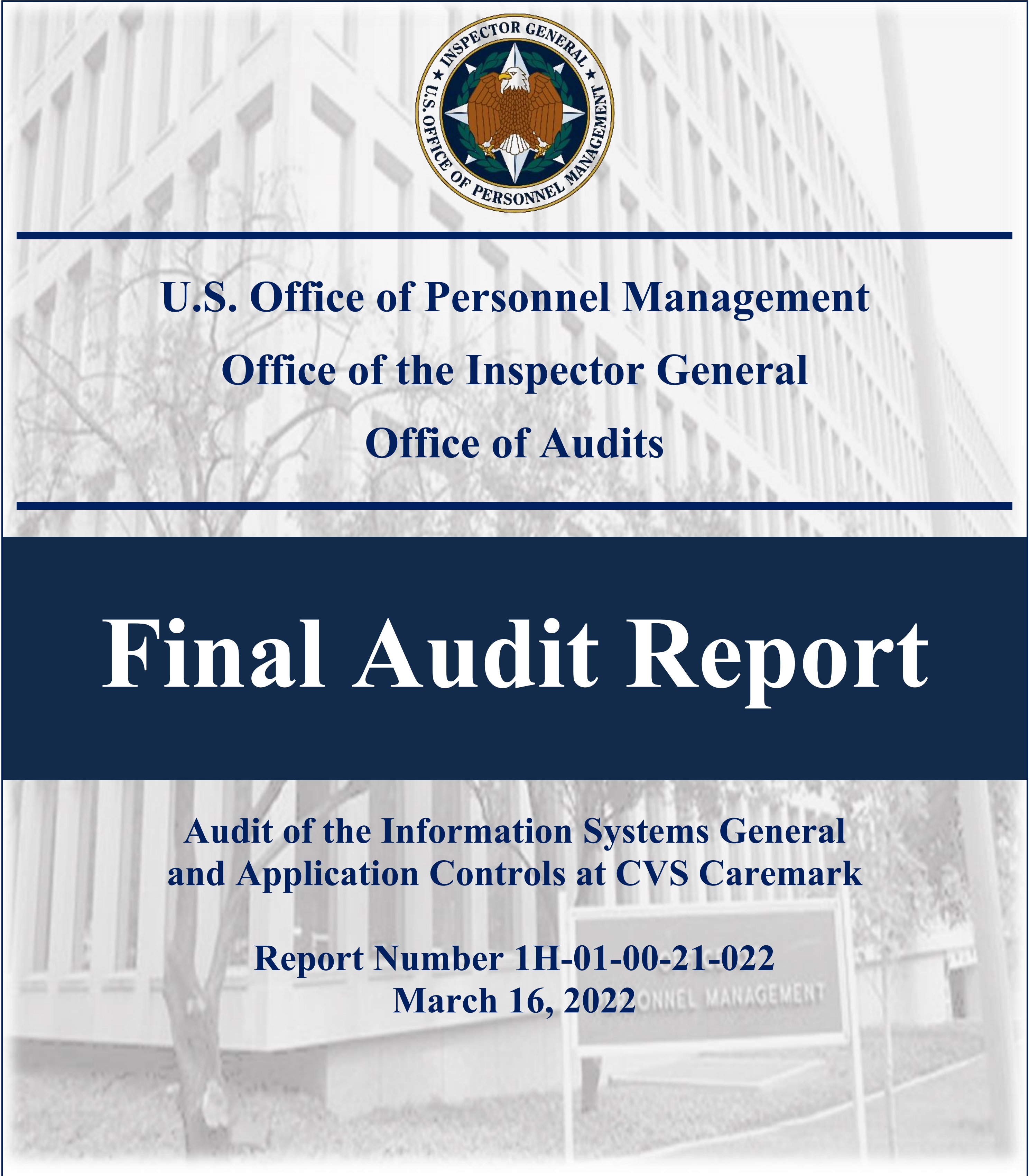

U.S. Office of Personnel Management

Office of the Inspector General

Office of Audits

Final Audit Report

Audit of the Information Systems General and Application Controls at CVS Caremark

Report Number 1H-01-00-21-022
March 16, 2022

Executive Summary

Audit of the Information Systems General and Application Controls at CVS Caremark

Report No. 1H-01-00-21-022 **March 16, 2022**

Why Did We Conduct the Audit?

CVS Caremark (CVS) is the pharmacy benefit manager responsible for processing prescription drug claims on behalf of several insurance carriers that contract 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 CVS's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by CVS to process and store data related to medical encounters and insurance claims for FEHBP members as of December 2021.

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of CVS's IT security controls determined that:

- An adequate security management program is implemented.
- Adequate physical and logical access controls are in place.
- Vulnerabilities discovered as a result of the vulnerability scan exercise require remediation.
- The enterprise security event monitoring and incident response programs are adequate.
- The contingency planning program is adequate.
- CVS has adequate application change control policies and procedures.

Abbreviations

CFR	**Code of Federal Regulations**
CVS	**CVS Caremark**
FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
GAO	**U.S. Government Accountability Office**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology Special Publication**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**

Table of Contents

I. Background

This 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 CVS Caremark (CVS).

The audit was conducted pursuant to FEHBP contracts CS 1039, CS 2962 and CS 1067; 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.

CVS is the pharmacy benefit manager responsible for processing prescription drug claims on behalf of the following FEHBP insurance carriers:

- Blue Cross Blue Shield Federal Employee Program (contract CS 1039);
- Government Employees Health Association (contract CS 2962); and
- National Association of Letter Carriers (contract CS 1067).

This was our second audit of the information technology (IT) general security and application controls at CVS. The previous audit of general and application controls at CVS was conducted in 2010. Final Audit Report No. 1H-01-00-10-057 was issued on May 17, 2011. All recommendations from the previous audit have been closed.

All CVS 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 CVS'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 CVS'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 CVS'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 CVS'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 CVS to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Scottsdale, Arizona.

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 CVS's information systems. The findings, recommendation, and conclusions outlined in this report are based on the status of information system general controls in place at CVS as of December 2021.

In conducting our audit, we relied to varying degrees on computer-generated data provided by CVS. 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 CVS'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 CVS'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 CVS's control structure. These criteria included, but were not limited to, the following publications:

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

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether CVS's practices were consistent with applicable standards. While generally compliant with respect to the items tested, CVS was not in complete compliance with all standards, as described in section III of this report.

III. Audit Findings and Recommendations

A. Security Management

The security management component of this audit involved an examination of the policies and procedures that serve as the foundation of CVS's overall IT security program. We evaluated CVS's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

CVS has developed adequate IT security policies and procedures, has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. CVS has also implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

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

CVS has adequate physical and logical access controls.

This audit included, but was not limited to, the following physical and logical access controls that were observed:

- Procedures for granting and removing access to CVS's facilities and data center;
- Procedures and policies for granting system and application access;
- Procedures and policies for removal and adjustment of system and application access; and
- Procedures and policies for the review and audit of logical access.

Nothing came to our attention to indicate that CVS has not implemented adequate prevention measures and controls related to 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 CVS'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:

- Perimeter controls to secure connections to external networks;
- Data loss prevention controls; and
- Network segmentation controls separating users from CVS's subnet of servers.

However, the following section documents an opportunity for improvement related to CVS's network security controls.

1. Vulnerability Management

CVS has some technical weaknesses in its IT environment.

CVS conducted credentialed vulnerability and configuration compliance scans on a sample of servers in its network environment on our behalf. We chose a sample of 254 servers from a universe of 4,765. The sample selection included a variety of system functionality and operating systems across production, test, and development. The judgmental sample was drawn from systems that store and/or process 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 CVS in the form of an audit inquiry, but will not be detailed in this report. CVS indicated that some of the vulnerabilities had been previously identified and have remediation plans or risk exceptions in place. However, there are still some vulnerabilities, [redacted]

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.

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

Recommendation 1: We recommend that CVS remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during audit fieldwork.

CVS's Response: ***"CVS agrees with Recommendation 1 and plans to implement the remediation to the specific technical weaknesses discovered during the audit in-line with our control remediation requirements no later than December 31, 2022."***

OIG Comments: As a part of the audit resolution process, we recommend that CVS provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence when it has fully implemented this recommendation.

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 CVS's security event monitoring and incident response programs identified the following controls in place:

- Controls in place for monitoring security events that occur in the network;
- Policies and procedures for analyzing and storing security events; and
- A documented incident response program.

Nothing came to our attention to indicate that CVS 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. CVS employs a team of technical personnel who manage system software configuration for the organization. We evaluated CVS's management of the configuration of its computer servers and databases.

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

- Documented configuration standards;
- Routine configuration reviews; and
- Documented system change control process.

Nothing came to our attention to indicate that CVS has not implemented adequate controls over its configuration management process.

F. Contingency Planning

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

CVS has adequate controls over contingency planning.

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

- Environmental controls to minimize disruptions;
- Documented contingency plans; and
- Documented contingency plan tests.

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

G. Application Change Control

We evaluated the policies and procedures governing CVS's application development and change control process.

CVS has implemented policies and procedures related to application configuration management and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- An adequately documented application change control process;
- Unit, integration, and user acceptance testing conducted in accordance with industry standards; and

- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that adequate controls have not been implemented over 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

February 2, 2022

Julius Rios, 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
CVS Caremark (CVS)
Audit Report Number 1H-01-00-21-022
(Dated Issued and Received on December 9, 2021)

The following represents the CVS'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

Vulnerability Management

Recommendation 1: We recommend that CVS remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during audit fieldwork.

Plan Response: CVS agrees with Recommendation 1 and plans to implement the remediation to the specific technical weaknesses discovered during the audit in-line with our control remediation requirements no later than December 31, 2022.

D. Security Event Monitoring and Incident Response

No recommendation noted.

E. Configuration Management

No recommendation noted.

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]

Sincerely,

[redacted]

[redacted]
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: 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