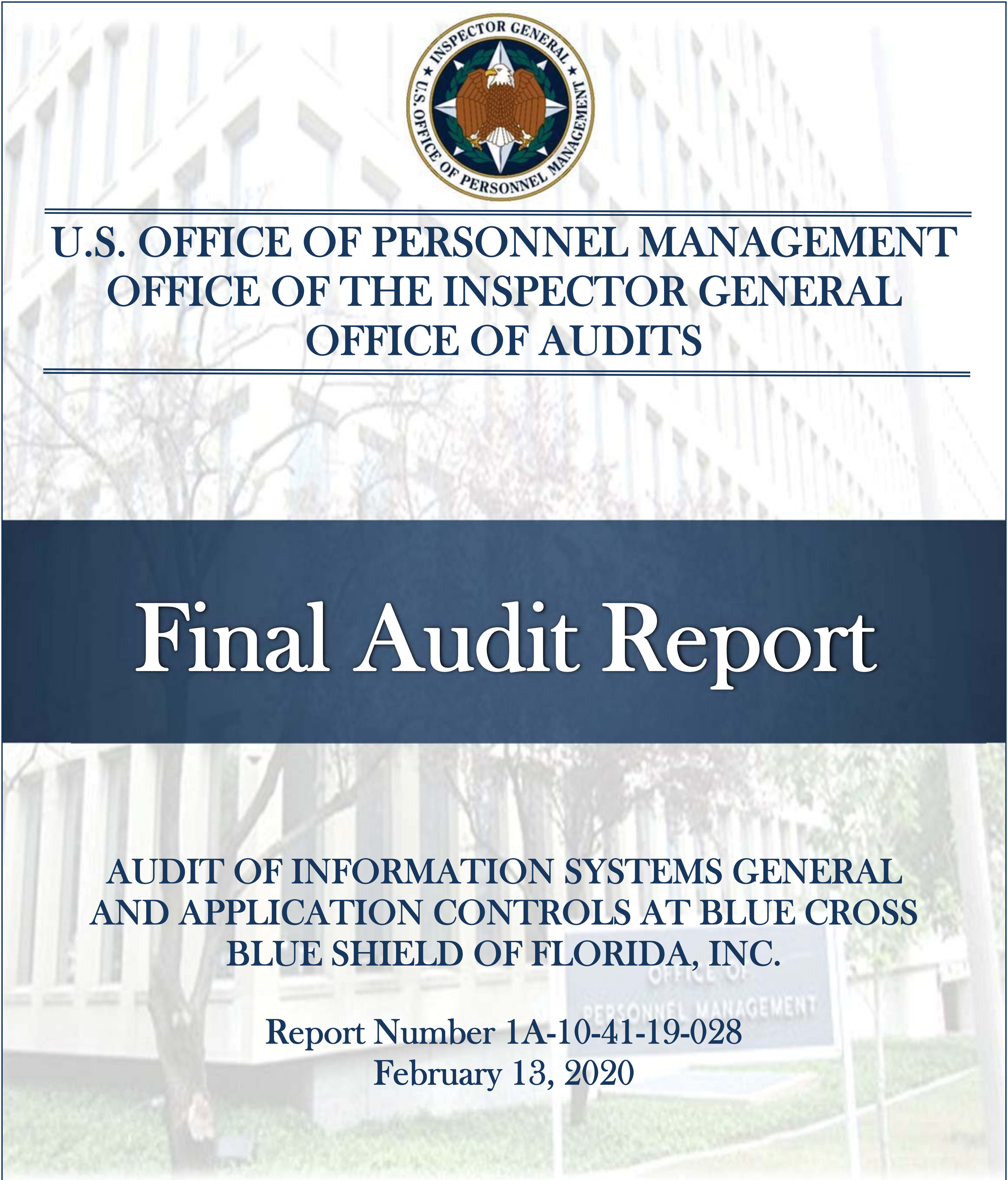

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF FLORIDA, INC.

Report Number 1A-10-41-19-028
February 13, 2020

EXECUTIVE SUMMARY

Audit of Information Systems General and Application Controls at Blue Cross Blue Shield of Florida, Inc.

Report No. 1A-10-41-19-028 **February 13, 2020**

Why Did We Conduct The Audit?

Blue Cross Blue Shield of Florida, Inc. (BCBSFL) 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 BCBSFL's information technology (IT) environment.

What Did We Audit?

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

- BCBSFL has an adequate security management program.
- Nothing came to our attention to indicate that BCBSFL has not implemented adequate controls over granting, removing, and monitoring access to facilities, network resources, and applications.
- [redacted]
- [redacted]
- [redacted]
- Adequate contingency planning controls are in place.
- BCBSFL has adequate policies and procedures in place related to claims adjudication.

ABBREVIATIONS

BCBSFL	**Blue Cross and Blue Shield of Florida, Inc.**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employees 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**
SLA	**Service Level Agreement**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 4

A. SECURITY MANAGEMENT 4

B. ACCESS CONTROLS 4

C. NETWORK SECURITY 5

1. Network Segmentation 5
2. OIG Vulnerability Scanning 6

D. CONFIGURATION MANAGEMENT 7

1. Security Configurations 7

E. CONTINGENCY PLANNING 8

F. CLAIMS ADJUDICATION 9

1. Application Change Control 9
2. Claims Processing System 10
3. Debarment 10

APPENDIX: BCBSFL's December 9, 2019, response to the draft audit report, issued October 9, 2019.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

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 Florida, Inc. (BCBSFL).

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, or comprehensive medical services.

This was our second audit of general and application controls at BCBSFL. The previous audit of general and application controls at BCBSFL was conducted in 2010. Final Audit Report No. 1A-10-41-09-063 was issued on May 21, 2010. All recommendations from the previous audit have been closed.

All BCBSFL 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 was 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 BCBSFL's IT environment. We accomplished these objectives by reviewing the following areas:

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

The onsite portion of this audit was performed in June and July of 2019. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at BCBSFL as of July 2019.

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

In conducting this audit we:

- Performed a risk assessment of BCBSFL'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 BCBSFL's business structure and environment; and

- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

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

- GAO's FISCAM;

- National Institute of Standards and Technology Special Publication (NIST SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy; and

- NIST SP 800-53, Revision 4, 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 BCBSFL's practices were consistent with applicable standards. While generally compliant with respect to the items tested, BCBSFL was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

BCBSFL has an adequate security management program.

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

BCBSFL has implemented a series of formal policies and procedures that govern its security management program. BCBSFL has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSFL has also implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

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

The access controls observed during this audit include, but are not limited to:

- Procedures for appropriately granting and removing physical access to facilities and data centers;

- Procedures for appropriately granting and adjusting logical access to applications and software resources; and

- Routine reviews of logical access to critical information.

Nothing came to our attention to indicate that BCBSFL has not implemented adequate controls over its access control process.

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 the BCBSFL network security program and reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Network access controls to prevent unauthorized devices from connecting to the internal network; and
- Documented policies and procedures to identify and respond to information security incidents.

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

1. Network Segmentation

BCBSFL uses [redacted]

[redacted]

[redacted]

[redacted]

Recommendation 1

We recommend that BCBSFL [redacted]

BCBSFL's Response:

"Florida Blue agrees with the OIG's observation. Florida Blue has an on-going project to [redacted]***. This implementation will be completed by March 31, 2020."***

OIG Comment:

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

2. OIG Vulnerability Scanning

We conducted credentialed vulnerability scans on a sample of servers in BCBSFL's network environment. [redacted]

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications.

[redacted]

Recommendation 2

We recommend that BCBSFL [redacted]

BCBSFL's Response:

[redacted]

OIG Comment:

BCBSFL has acknowledged the [redacted] We continue to recommend that BCBSFL follow through and remediate the [redacted]

D. 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. BCBSFL employs a team of technical personnel who manage system software configuration for the organization.

We evaluated BCBSFL's management of the configuration of its servers and databases.

Our review found the following controls in place:

- Documented system change control process;
- Established patch management process; and
- Formally documented and approved security configuration standards.

The following section documents an opportunity for improvement related to BCBSFL's configuration management program.

1. Security Configurations

[redacted]

[redacted]

NIST SP 800-53, Revision 4, states that an organization must develop, document, and maintain a current baseline configuration of the information system.

[redacted]

Recommendation 3

We recommend that BCBSFL apply [redacted]

BCBSFL's Response:

"Florida Blue agrees with OIG's observation. [redacted]

E. CONTINGENCY PLANNING

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

BCBSFL has adequate contingency planning controls in place.

- Environmental controls to minimize disruptions;
- Disaster recovery plan (e.g., recovery of hardware and software infrastructure); and
- Disaster recovery plan tests.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems."

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

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSFL's claims adjudication process. [redacted] We reviewed the following processes related to claims adjudication: application configuration management, claims processing, and provider debarment.

1. Application Change Control

We evaluated the policies and procedures governing application development and change control over BCBSFL's claims processing system.

BCBSFL 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:

- Documented application change control process;
- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and
- [redacted]

Nothing came to our attention to indicate that adequate controls have not been implemented over the application configuration management process.

2. Claims Processing System

BCBSFL has sufficient input, processing, and output controls over claims processing.

We evaluated the business process controls associated with BCBSFL's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that BCBSFL has implemented policies and procedures to help ensure that:

- [redacted]
- [redacted]
- [redacted]

Nothing came to our attention to indicate that BCBSFL has not implemented adequate controls over its claims processing system.

3. Debarment

BCBSFL has documented procedures for reviewing provider files for debarments and suspensions. [redacted]

Nothing came to our attention to indicate that BCBSFL has not implemented adequate controls over the debarment 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

December 9, 2019

[redacted], 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
Blue Cross Blue Shield of Florida (Florida Blue)
Audit Report Number 1A-10-41-19-028
(Dated October 9, 2019)

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

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

No recommendation noted.

C. NETWORK SECURITY

1. Network Segmentation

Recommendation 1

We recommend that Florida Blue [redacted]

Plan Response

Florida Blue agrees with the OIG's observation. Florida Blue has an on-going project to [redacted]. This implementation will be completed by March 31, 2020.

2. OIG Vulnerability Scanning

Recommendation 2

We recommend that Florida Blue [redacted]

Plan Response

[redacted]

D. CONFIGURATION MANAGEMENT

1. Security Configurations

Recommendation 3

We recommend that Florida Blue [redacted]

Plan Response

Florida Blue agrees with the OIG’s observation. [redacted]

E. CONTINGENCY PLANNING

No recommendation noted.

F. Claims Adjudication

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] [redacted] or [redacted] at [redacted].

Sincerely,

[redacted]

Managing Director, FEP Program Assurance

cc: [redacted], OPM
[redacted], OPM
[redacted], FEP
[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