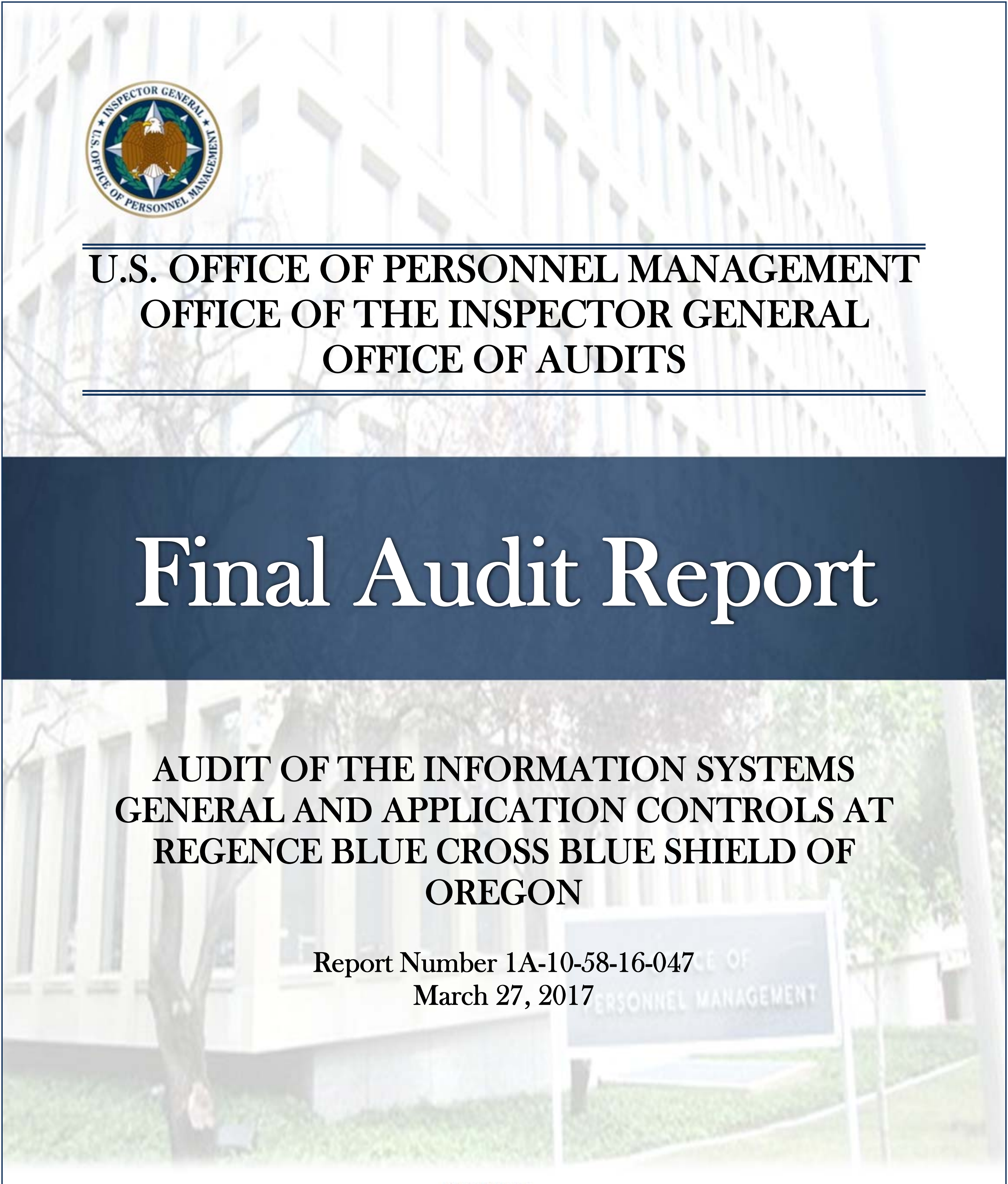

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT REGENCE BLUE CROSS BLUE SHIELD OF OREGON

Report Number 1A-10-58-16-047
March 27, 2017

-- CAUTION --

This report has been distributed to Federal officials who are responsible for the administration of the subject program. This non-public version may contain confidential and/or proprietary information, including information protected by the Trade Secrets Act, 18 U.S.C. § 1905, and the Privacy Act, 5 U.S.C. § 552a. Therefore, while a redacted version of this report is available under the Freedom of Information Act and made publicly available on the OIG webpage (http://www.opm.gov/our-inspector-general), this non-public version should not be further released unless authorized by the OIG.

EXECUTIVE SUMMARY

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

Report No. 1A-10-58-16-047 **March 27, 2017**

Why Did We Conduct the Audit?

Regence Blue Cross Blue Shield of Oregon (Regence) 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 Regence's information technology (IT) environment.

What Did We Audit?

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

- Regence has established an adequate security management program.
- Regence has implemented controls to prevent unauthorized physical access to its facilities. However, logical access controls could be improved by implementing multi-factor authentication for privileged users.
- Regence has implemented an incident response and network security program. Regence has also implemented preventative controls at the network perimeter and performs security event monitoring throughout its network. However, Regence has not implemented network access controls throughout the entire facility. Regence has also not documented an approved firewall security configuration standard.
- Regence has developed and documented formal configuration management policies and configuration standards for its operating platforms.
- Regence's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications. Regence also tests these plans on a routine basis.
- Regence has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately.

This report is non-public and should not be further released unless authorized by the OIG, because it may contain confidential and/or proprietary information that may be protected by the Trade Secrets Act, 18 U.S.C. § 1905, or the Privacy Act, 5 U.S.C. § 522a.

ABBREVIATIONS

BCBSA	**Blue Cross Blue Shield Association**
Cambia	**Cambia Health Solutions**
CFR	**Code of Federal Regulations**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**Federal Employee Program**
FISCAM	**Federal Information Security 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**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
Regence	**Regence Blue Cross Blue Shield**

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 Regence Blue Cross Blue Shield of Oregon (Regence).

The audit was conducted pursuant to FEHBP contracts 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 first audit of Regence's information technology (IT) general and application controls. All Regence 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 Regence's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation management;
- Contingency planning; and
- Application controls specific to Regence'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 Regence'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 Regence'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 Regence to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Portland, Oregon.

Regence is a subsidiary of Cambia Health Solutions (Cambia), which offers a wide range of insurance products and services. All of the information technology (IT) functions at Regence are managed by Cambia. The operations of Cambia were considered within the scope of this audit.

Regence is a subsidiary of Cambia Health Solutions. The operations of Cambia are within the scope of this audit.

The on-site portion of this audit was performed in June and July of 2016. 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 Regence as of July, 2016.
In conducting our audit, we relied to varying degrees on computer-generated data provided by Regence. 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 review we:

- Gathered documentation and conducted interviews;

- Reviewed Regence’s business structure and environment;

- Performed a risk assessment of Regence’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); 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 for evaluating Regence’s control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;

- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;

- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;

- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;

- GAO's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, An Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- 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;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

As mentioned above, Regence is a subsidiary of Cambia. Therefore, all Cambia policies and procedures related to information security management apply to Regence. The security management component of this audit involved the examination of the policies and procedures that are the foundation of Cambia's overall IT security program. We evaluated Cambia's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Cambia maintains a series of thorough IT security policies and procedures applicable to Regence.

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

Nothing came to our attention to indicate that Cambia 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 of Regence's and Cambia's facilities and data center. We also examined the logical controls protecting sensitive data on Cambia's network environment and claims processing related 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 the data center;

- Procedures for appropriately granting, adjusting, and removing logical access;

- Routinely reviewing user access; and

- Adequate environmental controls over the data center.

The following section documents one opportunity for improvement related to Cambia's logical access controls.

1. Privileged User Authentication

Access to privileged user (system administrator) accounts at Cambia requires multi-factor authentication when [redacted] We expect all FEHBP contractors to require multi-factor authentication for administrator-level access to information systems regardless of where the user is physically located. Cambia currently has a project in progress to fully enforce multi-factor authentication for system administrators. However, the control had not been implemented at the time of our audit fieldwork.

The Federal government requires multi-factor authentication for all information system users. Although Cambia is not a government entity, it does process sensitive healthcare data of Federal employees. Therefore, we recommend that Cambia implement this control for privileged users at a minimum. NIST SP 800-53, Revision 4, states that information systems should implement multi-factor authentication for network access to privileged accounts. Failure to implement multi-factor authentication increases the risk that privileged user credentials could be compromised and that unauthorized users could access sensitive and proprietary data.

Recommendation 1

We recommend that Regence/Cambia require multi-factor authentication for privileged user access to all information systems.

Regence/Cambia Response:

"Cambia agrees with this recommendation. As noted in the report, a project is underway to implement multifactor authentication for privileged user access to information systems that store or process Personal Health Information (PHI). Cambia anticipates completion of this effort by [redacted]."

OIG Comment:

As a part of the audit resolution process, we recommend that Regence/Cambia provide OPM's Healthcare and Insurance Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement applies to subsequent recommendations in this audit report that Regence/Cambia agrees to implement.

C. NETWORK SECURITY

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Regence/Cambia does not have a formal firewall configuration standard.

We evaluated Cambia's network security program and reviewed the results of several automated vulnerability scans that we independently performed during this audit. We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network;
- An adequate vulnerability management program; and
- A documented incident response program.

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

1. Documented Firewall Standard

Cambia's network has firewall devices installed at key locations on the network perimeter and between internal logical security zones. However, Cambia has not formally documented a policy or standard that identifies the types of traffic allowed by the organization and the approved settings that are needed to harden firewalls within the network.

NIST SP 800-41, Revision 1, states that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies."

Cambia conducts routine reviews of its firewalls' rule bases, and also performs vulnerability scans capable of detecting firewall configuration insecurities. However, this process could be further improved by creating an approved firewall security configuration standard. This will enable Cambia to routinely audit the current/actual settings of its firewalls against the approved settings. Failure to routinely review actual firewall configuration settings and compare them to approved settings could potentially increase the organization's exposure to insecure traffic and vulnerabilities.

Recommendation 2

We recommend that Regence/Cambia develop a formal firewall configuration standard, and that this standard be used to perform routine firewall configuration audits.

Regence/Cambia Response:

"Cambia agrees with this recommendation. A variety of configuration standards are currently used in the building and maintenance of our firewalls. The development of a formal security standard for firewalls is underway. Cambia anticipates completion of this effort by [redacted]."

2. Network Access Control

Cambia has implemented network access controls in its shared conference rooms that prevent non-authorized computing devices from connecting to the company's internal network. [redacted] This security approach relies on physical access controls to prevent unauthorized personnel from accessing the facilities and connecting unauthorized devices to the network. While Regence and Cambia's physical access controls are robust, they cannot be considered impenetrable, and therefore we believe that additional logical controls would add value. Furthermore, Cambia's current control structure does not prevent employees with valid physical access to its facilities from connecting their own unauthorized devices (e.g., a personal device) to the network.

NIST SP 800-53, Revision 4, states that information systems should uniquely identify and authenticate devices before establishing a network connection.
Failure to control access to network ports could allow unauthorized users or devices to connect to sensitive network resources.

Recommendation 3

We recommend that Regence/Cambia implement network access controls [redacted]

Regence/Cambia Response:

"Cambia agrees with this recommendation. Cambia will develop a project plan for this effort by [redacted], with a targeted pilot implementation (as defined in the project plan) to complete by [redacted]. A final full implementation completion date will be provided at the conclusion of the pilot implementation phase."

D. CONFIGURATION MANAGEMENT

A configuration management program is the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated Cambia's configuration management program and observed the following controls in place:

- A thorough change management process;

- Documented technical configuration standards; and

- Routine configuration compliance reviews.

Nothing came to our attention to indicate that Cambia does not have an adequate configuration management program.

E. CONTINGENCY PLANNING

We reviewed the following elements of Cambia's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur:

Regence/Cambia maintains and routinely tests its disaster recovery and business continuity plans.

- Disaster recovery plan;

- Business continuity plan;
- Contingency plan tests; and
- Emergency response procedures.

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.” Cambia has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

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

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting the Regence claims adjudication process. Regence processes all FEHBP claims through the Blue Cross Blue Shield Association’s (BCBSA) FEP (Federal Employee Program) Direct nationwide claims adjudication system. Regence uses a local claims processing system for its other lines of business, but relies on the controls and edits within FEP Direct for FEHBP claims.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of Regence’s claims processing systems.

Cambia has documented system development life cycle procedures that IT personnel follow during routine software modifications. All changes require approval and undergo testing prior to migration to the production environment.

Nothing came to our attention to indicate that Cambia has not implemented adequate controls over application configuration management.

2. Claims Processing System

We evaluated the input, processing, and output controls associated with Regence's claims processing system. We determined that Regence has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail processing facilities are tracked to ensure timely processing;

- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and

- Claims scheduled for payment are actually paid.

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

3. Debarment

Regence has adequate procedures for updating its claims system with debarred provider information. Regence is notified by BCBSA that an update to the OPM OIG debarment list is available. Plan personnel review the list to determine if any debarred providers have active contracts with Regence. If an active provider is determined to be debarred, the provider is flagged in FEP Direct, which will cause any incoming claims to defer for further review. Regence adheres to the OPM OIG debarment guidelines to include initial member notification, a 15-day grace period, and then denial of subsequent claims.

Nothing came to our attention to indicate that Regence has not implemented adequate controls over the debarment process.

4. Application Controls Testing

Regence processes all FEHBP claims directly through the BCBSA's FEP Direct nationwide claims adjudication system. We conducted a test on FEP Direct to evaluate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which the claims processing system adjudicated the claims.

Our test work did not identify any new issues with FEP Direct. All issues encountered during this audit have been previously reported to the BCBSA through recommendations on other audit reports.

APPENDIX

December 2, 2016

[redacted]
Chief, Information Systems Audit Group
U.S. Office of Personnel Management (OPM)
1900 E Street, Room 6400
Washington, D.C. 20415-1100

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

Reference OPM DRAFT IT AUDIT REPORT
Regence Blue Cross Blue Shield of Oregon
Audit Report Number 1A-10-58-16-047
(Dated September 30, 2016)

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

A. Network Security

No recommendation noted.

B. Access Controls

1. Privileged User Authentication

<u>Recommendation 1</u>

We recommend that Regence/Cambia require multi-factor authentication for privileged user access to all information systems.

<u>Plan Response</u>

Cambia agrees with this recommendation. As noted in the report, a project is underway to implement multifactor authentication for privileged user access to information systems that store or process Personal Health Information (PHI). Cambia anticipates completion of this effort by [redacted].

C. Network Security

2. Documented Firewall Standard

Recommendation 2

We recommend that Regence/Cambia develop a formal firewall configuration standard, and that this standard be used to perform routine firewall configuration audits.

Plan Response

Cambia agrees with this recommendation. A variety of configuration standards are currently used in the building and maintenance of our firewalls. The development of a formal security standard for firewalls is underway. Cambia anticipates completion of this effort by [redacted].

3. Network Access Control

Recommendation 3

We recommend that Regence/Cambia implement network access controls on all ports throughout its facilities.

Plan Response

Cambia agrees with this recommendation. Cambia will develop a project plan for this effort by [redacted], with a targeted pilot implementation (as defined in the project plan) to complete by [redacted]. A final full implementation completion date will be provided at the conclusion of the pilot implementation phase.

D. Configuration Management

No recommendations noted.

E. Contingency Planning

No recommendations noted.

F. Claims Adjudication

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 [redacted] at [redacted].

Sincerely,

[redacted]

[redacted]
Managing Director, FEP Program Assurance

cc: [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

-- CAUTION --

This report has been distributed to Federal officials who are responsible for the administration of the subject program. This non-public version may contain confidential and/or proprietary information, including information protected by the Trade Secrets Act, 18 U.S.C. § 1905, and the Privacy Act, 5 U.S.C. § 552a. Therefore, while a redacted version of this report is available under the Freedom of Information Act and made publicly available on the OIG webpage (*http://www.opm.gov/our-inspector-general*), this non-public version should not be further released unless authorized by the OIG.